UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MINNESOTA

Odom Sports Medicine P.A. d/b/a Odom Health & Wellness, on behalf of itself and all others similarly situated,

Plaintiff,

v.

UnitedHealth Group Incorporated, UnitedHealthCare Services, Inc., Optum Insight, Change Healthcare Inc., Change Healthcare Operations, LLC, Change Healthcare Solutions, LLC, Change Healthcare Holdings, Inc., Change Healthcare Technologies, LLC, and Change Healthcare Pharmacy Solutions, Inc., Optum, Inc., Optum Financial, Inc., Optum Bank, and Optum Pay,

Defendants.

Case No. 0:25-cv-949

CLASS ACTION COMPLAINT AND JURY DEMAND

TABLE OF CONTENTS

Plaintiff Odom Sports Medicine P.A. d/b/a Odom Health & Wellness ("Plaintiff"), on behalf of itself and all others similarly situated, brings this class action complaint against Defendants UnitedHealth Group Incorporated ("UHG"), UnitedHealthCare Services, Inc. ("UHCS"), Optum Insight, Change Healthcare Inc. ("Change Healthcare"), Change Healthcare Operations, LLC ("CHO"), Change Healthcare Solutions, LLC ("CHS"), Change Healthcare Holdings, Inc. ("CHH"), Change Healthcare Technologies, LLC ("CHT"), and Change Healthcare Pharmacy Solutions, Inc. ("CHPS") (Change Healthcare, CHO, CHS, CHH, CHT, and CHPS together, referred to as "Change") (Change, with UHG, UHCS, and Optum Insight, the "Change Health Defendants"). Plaintiff, on behalf of itself and all others similarly situated, also brings this class action complaint against Optum, Inc., Optum Financial, Inc. ("Optum Financial"), Optum Bank, and Optum Pay, (collectively, the "Optum Financial Defendants") (Change Health Defendants and the Optum Financial Defendants, together, "Defendants"). Plaintiff makes the following allegations:

PRELIMINARY STATEMENT

1. The Change Health Defendants control the largest healthcare payment platform in United States (the "Change Platform"), providing, among other things, a claims processing service that is used by healthcare providers and pharmacies ("Providers") to submit claims to insurance companies and receive reimbursement for services performed (the "Services"). The Change Platform processes 15 billion transactions annually, "touching one in three U.S. patient records."[1] In dollar terms, the Change Platform

[1] Nicole Sganga & Andres Triay, *Cyberattack on UnitedHealth still impacting prescription access:*

processes approximately "$2 trillion in health care payments each year," meaning Change is "responsibl[e] for more than 44% of all the dollars flowing through the health care system."[2]

2. To operate the Change Platform, Change Health Defendants transact in and store huge volumes of confidential information including highly sensitive and confidential patient information including full names, phone numbers, addresses, Social Security numbers, emails, and payment information, referred to "Personally Identifying Information" or "PII." They also store patients' medical records, claims information, provider information, diagnoses, medicines, test results, images, care and treatment, and billing, claims and payment information including health insurance information (such as health plans and policies, insurance companies, member and group ID numbers, and Medicaid-Medicare-government payer ID numbers)—collectively known as "Private Health Information" or "PHI" (PII and PHI together are referred to as "Private Information").

3. In February 2024, as a direct result of Change Health Defendants' failure to employ even rudimentary cybersecurity precautions to authenticate the identities of people logging in to their networks, Change Health Defendants' systems were compromised in the

"These are threats to life," CBS NEWS (Feb. 29, 2024, 9:00 PM), https://www.cbsnews.com/news/unitedhealth-cyberattack-change-healthcare-prescription-access-still-impacted/ (last visited Jan. 14, 2024).

[2] *American Hospital Association Letter to Congress*, American Hospital Association (Apr. 29, 2024), https://www.aha.org/system/files/media/file/2024/04/24-04-29-AHALTRtoEandConUHG-webwattachment.pdf at 1 (last visited Jan. 14, 2025).

largest health care ransomware attack in history (the "Ransomware Attack"), which compromised millions of patients' Private Information.

4. In the aftermath of the Ransomware Attack, Change Health Defendants' systems were left in gross disrepair. Change Health Defendants had no viable backup plans or systems. And in a largely futile effort to prevent further collapse of its systems, Change Health Defendants elected to take the remaining systems—including the Change Platform—offline completely, rendering it useless to Providers.

5. While the Change Platform was shut down, Providers were unable to verify insurance, determine copays, submit claims, or receive payment. As a result, Providers did not timely receive *billions* of dollars in earned reimbursements. The impact on the U.S. health care system, and particularly Providers, was devastating. Hospitals, clinics, doctors, and therapists were left without a mechanism to be paid for their services for months. Likewise, pharmacies were unable to use the Change Platform to confirm patients' insurance coverage, putting pharmacies in the position of not being able to determine what to charge patients for vital medications. Pharmacists were left unable to fill prescriptions for many patients, including patients who could not, or would not, cover the full cost of prescriptions. According to John Riggi, national advisor for cybersecurity and risk at the American Hospital Association ("AHA"), "this cyberattack has affected every hospital in the country one way or another."[3]

[3] Nicole Sganga & Andres Triay, *Cyberattack on UnitedHealth still impacting prescription access: "These are threats to life,"* CBS NEWS (Feb. 29, 2024, 9:00 PM), https://www.cbsnews.com/news/unitedhealth-cyberattack-change-healthcare-prescription-access-still-impacted/ (last visited Jan. 14, 2025).

6. During the shutdown, many Providers were unable to verify patient eligibility and coverage, file claims, appeal denials or partial denials of claims, receive electronic health remittances (ERAs), bill patients, or receive payments from insurers.[4] This continued for nearly three months, when many Providers received little, if any, reimbursement from insurers for patient visits. Without reimbursement, many Providers were not able to afford employee payroll, make rent and mortgage payments, and secure medical supplies. At the same time, Providers had to bring on new staff and divert and pay existing staff overtime in order to attempt manual claim submissions or use other workarounds to seek payment. Many Providers took out high-interest loans to cover costs during the Change Platform shutdown.

7. Exacerbating this crisis, Change Health Defendants did not provide adequate transparency and guidance to Providers during the shutdown. Specifically, Change Health Defendants published misleading statements with significant omissions during the shutdown to lead Providers and the public to believe that the Change Platform would be offline only briefly. These statements were designed to pacify Providers to keep them from defecting to competitors and to hide Change Health Defendants' incompetence from the public—all while Change Health Defendants knew that the outage would continue for much longer. Almost a year after the Ransomware Attack and a claimed $2.5 billion in remediation costs, Change Health Defendants still have not fully restored their systems.

[4] *See* Associated Press, *Minnetonka Based United Healthcare Hacked*, KNSI (Feb. 29, 2024, 5:46 PM), https://knsiradio.com/2024/02/29/minnetonka-based-united-healthcare-hacked/ (last visited Jan. 14, 2025).

8. Since the Ransomware Attack and shutdown, it has come to light that, despite the known risks of ransomware attacks to the healthcare industry, Change Health Defendants failed to implement reasonable security procedures and practices and failed to disclose material facts surrounding their deficient security protocols. Change Health Defendants have admitted that a well-known ransomware gang—ALPHV—was able to enter their externally facing server because it was not protected with even basic multifactor authentication ("MFA"). But there were multiple other critical failures. As Senator Wyden exclaimed during the Senate hearing, "the attack could have been stopped with Cybersecurity 101."[5]

9. As a result of Defendants' conduct, Providers have suffered and will continue to suffer substantial harm. The event pushed many Providers to the brink of closure (and forced some Providers to close altogether). To survive, Providers necessarily incurred extra costs to make up for unpaid claims and in an attempt to submit claims without the Change Platform. Moreover, Providers will never see any compensation for claims that they were unable to submit during the shutdown. As explained below, almost a year after the Ransomware Attack, Providers are still in a precarious financial situation due to Defendants' conduct and failures.

10. In an effort to stem the devastating tide of financial harm caused by their failures, Defendants offered a "Temporary Funding Assistance Program" (TFAP) to

[5] Pietje Kobus, *UnitedHealth CEO Testifies on Cyberattack Before Senate*, HEALTHCARE INNOVATION (May 2, 2024), https://www.hcinnovationgroup.com/cybersecurity/news/55036427/unitedhealth-ceo-testifies-on-cyberattack-before-senate (last visited Jan. 14, 2025).

Providers, a program which, according to Defendants, has provided billions of dollars in loans to Providers.

11. However, even though Providers are still financially reeling in the wake of the Ransomware Attack, and despite a promise not to collect until Providers were made whole, Defendants are now demanding full repayment of those loans, often in a single lump sum.

12. As alleged below, Plaintiff seeks redress for Defendants' conduct.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. There are more than 100 putative Class members and at least some members of the proposed Classes have a different citizenship from Defendants. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367 because all claims alleged herein form part of the same case or controversy.

14. On June 7, 2024, the Judicial Panel on Multidistrict Litigation issued an order centralizing litigation arising from the Ransomware Attack in this District. MDL Pretrial Order No. 1 (ECF 54) allows Plaintiff to directly file this case in the MDL docket.

15. The District of Minnesota may exercise jurisdiction over Defendants because they maintain their principal place of business in Minnesota, are registered to conduct business in Minnesota, have sufficient minimum contacts in Minnesota, have consented to jurisdiction in Minnesota; and/or, intentionally availed themselves of the markets within

Minnesota through the promotion, sale, and marketing of the Services, thus rendering the exercise of jurisdiction by this Court proper and necessary.

16. Venue is proper in the District of Minnesota under 28 U.S.C. § 1391 because Defendants UHG, UHCS, Optum, Inc., Optum Financial, Optum Insight, and CHT reside in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

I. Defendants

17. Defendant UnitedHealth Group Incorporated is a Delaware corporation with its principal place of business in Minnetonka, Minnesota, and is registered to do business in the State. UHG exercises control over the management of the Change cybersecurity systems as evidenced by, inter alia, UHG's response to the Ransomware Attack as alleged herein.

18. UHG "is a vertically integrated healthcare company" comprised of non-defendant United Healthcare Insurance Co. ("UHIC"), the largest commercial health insurer in America, and three Optum divisions: Optum Health, Optum Insight, and Optum Rx.[6] UHG "is a health care leviathan" that, in 2023, "generated $324 billion in revenue, making it the fifth largest company in America."[7] Its sprawling corporate structure is shown in **Exhibit A**.

---

[6] *U.S. v. UnitedHealth Group Inc., and Change Healthcare Inc.*, 1:22-cv-481, Def.'s Proposed Findings of Fact and Conclusions of Law, Dkt. No. 121 at 3 (D.D.C. Sept. 7, 2022).

[7] *Opening Statement Testimony of Senator Ron Wyden*, Senate Finance Committee (May 1, 2024), https://www.finance.senate.gov/imo/media/doc/0501_wyden_statement.pdf at 1 (last visited Jan. 14, 2025).

19. Defendant UnitedHealthCare Services, Inc. is a direct subsidiary of UHG and maintains its principal place of business in Minnetonka, Minnesota, and is incorporated and registered to do business in Minnesota. UHCS is the parent to UHG's insurance business (UHIC), and healthcare services business operated under the Optum brand. UHG describes UHCS as providing "administrative services."[8] On the repayment demand letters sent to Providers that took out TFAP loans, Providers are directed to send payment to UHCS.

20. Defendant Optum Insight, Inc. is a direct subsidiary of UHCS. It is incorporated in Delaware, and has its principal place of business in Eden Prairie, Minnesota. Optum Insight is registered to do business in Minnesota. Optum Insight is "a data and technology company and a technology-enabled services business" that offers a range of solutions including data, analytics, research, consulting, technology, and managed services to hospitals, physicians, health plans, governments, and life sciences companies.[9] According to Change Healthcare Defendants, Optum Insight assists customers in lowering administrative expenses, complying with regulations, enhancing clinical performance, and reimagining operational processes.[10] When some Providers attempted to contact Change Healthcare for help during the prolonged shutdown, they received responses from Optum Insight.

---

[8] Legal Entities, UnitedHealthcare, www.uhc.com/legal/legal-entities (last visited Jan. 6, 2025).
[9] *U.S. v. UnitedHealth Group Inc., and Change Healthcare Inc.*, 1:22-cv-481, Post-Trial Memorandum Opinion, Dkt. No. 138 at 11 and 18 (D.D.C. Sept. 21, 2022).
[10] *Optum: Technology and data-enabled care delivery*, UNITEDHEALTH GROUP, https://www.unitedhealthgroup.com/people-and-businesses/businesses/optum.html (last visited Jan. 14, 2025).

21. Defendant Change Healthcare Inc. is a subsidiary of UHG, and is incorporated in Delaware, with its principal place of business in Nashville, Tennessee. Change Healthcare is now operated as part of Optum Insight and maintained the Change Platform at all relevant times.

22. Defendant Change Healthcare Operations, LLC is a subsidiary of Change Healthcare. It is incorporated in Delaware, with its principal place of business in Nashville, Tennessee. CHO is a contracting entity for Change Healthcare.[11] In order to acquire a TFAP loan, Providers were required to enter an agreement with CHO.

23. Defendant Change Healthcare Solutions, LLC is a subsidiary of or "managed" by CHO. It is incorporated in Delaware, has its principal place of business in Nashville, Tennessee, and is registered to do business in Minnesota. CHS provides "software & services for health plans & providers,"[12] and is one of the contracting entities for Providers to access the Change Platform.

24. Defendant Change Healthcare Holdings, Inc. is a subsidiary of Change Healthcare. CHH is incorporated in Delaware, with its principal place of business in Nashville, Tennessee. In Defendant CHT's Minnesota Secretary of State Business registration, CHH's address is listed as Optum's headquarters in Eden Prairie, Minnesota.

---

[11] *See, e.g.*, https://www.gsaelibrary.gsa.gov/ElibMain/home.dohttp:/www.gsaelibrary.%20gsa.gov/ElibMain/contractClauses.do?scheduleNumber=MAS&contractNumber=GS-35F-0176X&contractorName=CHANGE+HEALTHCARE+OPERATIONS%2C+LLC&duns=C7DYEBLK3PE1&source=ci&view=clauses (last accessed Jan. 6, 2025).

[12] Vendor Profile – Change Healthcare Solutions, LLC, https://oregonbuys.gov/bso/external/vendor/vendorProfileOrgInfo.sdo?external=true&vendorId=V00019459 (last visited Jan. 6, 2025).

25. Defendant Change Healthcare Technologies, LLC is a subsidiary of, or "managed" by, CHH. It is incorporated in Delaware, and is registered to do business in Minnesota, and on such registration lists a principal place of business in Eden Prairie, Minnesota. CHT is a contracting entity for Change Healthcare and is one of the contracting entities for Providers to access the Change Platform.[13]

26. Defendant Change Healthcare Pharmacy Solutions, Inc. is a subsidiary of Change Healthcare. It is incorporated in Maine, with a principal place of business in Nashville, Tennessee. CHPS is registered to do business in Minnesota. It describes itself as providing "Pharmacy Benefit Administration,"[14] and as a "Pharmacy Benefits Manager,"[15] and is one of the contracting entities for Providers to access the Change Platform.

27. Defendant Optum, Inc. is a subsidiary of UHCS. It is incorporated in Delaware. Optum, Inc. has its principal place of business in Eden Prairie, Minnesota, and is registered to do business in Minnesota. It "functions as a holding company for the health services business."[16] The letters sent to Providers demanding repayment of TFAP loans have been sent on Optum letterhead.

---

[13] *See, e.g.*, https://www.osc.ny.gov/files/state-agencies/contracts/xreports/2022/forma/SNY01-C505573-3320211.pdf (last accessed Jan. 6, 2025), https://www.hca.wa.gov/assets/program/k6038-chc-mra-redacted.pdf (last accessed Jan. 6, 2025).

[14] Vendor Profile – Change Healthcare Pharmacy Solutions, Inc., https://www.bidbuy.illinois.gov/bso/external/vendor/vendorProfileOrgInfo.sdo?external=true&vendorId=V00010940 (last visited Jan. 6, 2025).

[15] Company List Report, May 22, 2023, https://www.wvinsurance.gov/Portals/0/PBM%20List%205-22-23.pdf (last accessed Jan. 14, 2025).

[16] *Id.*

28. Defendant Optum Financial, Inc. is a subsidiary of Optum, Inc. It is incorporated in Delaware, with a principal place of business in Eden Prairie, Minnesota. Optum Financial is registered to do business in Minnesota. It describes itself as providing solutions for "people and organizations [to] save, spend, invest, and pay for health care."[17]

29. Defendant Optum Bank is a subsidiary of Optum Financial. It is incorporated, and has its principal place of business, in Utah. It is a member of the FDIC, and "offer[s] or administer[s]"[18] HSAs, FSAs, HRAs, MSAs, and other health accounts, for Optum Financial.

30. Defendant Optum Pay is a "financial solution" "platform that helps expedite payments," "optimize claims reconciliation," and allows "[P]roviders [to] choose how to receive payments from a network of payers."[19] Optum Pay is "made possible by Optum Financial, Inc. and its subsidiaries" and related "[b]anking services are provided by OptumBank."[20] Providers were required to access TFAP loans through an Optum Pay account and managed their loans from that same account.

II. UHG's Acquisition of Change Healthcare

31. Change Healthcare was founded in 1996 and provides data solutions to health insurers and providers to facilitate clinical decision making and payment processing across

[17] Financial Solutions, UnitedHealth Group, www.unitedhealthgroup.com/uhg/what-we-do/health-financial-services.html (last visited Jan. 6, 2025).
[18] Optum Bank, www.optumbank.com (last visited Jan. 6, 2025).
[19] Financial Solutions, Payments and lending, Optum Pay, www.business.optum.com/en/financial-solutions/payments-lending-solutions/optum-pay.html (last visited Jan. 6, 2025).
[20] Optum Pay Premium Sell Sheet, available at https://www.optum.com/content/dam/o4-dam/resources/pdfs/sell-sheets/optum-pay-premium-sell-sheet.pdf (last accessed Jan. 6, 2025).

the healthcare industry.[21] In 2017, Change Healthcare entered into a joint venture with McKesson Corporation's Technologies Solutions Division. In January 2021, UHG agreed to purchase Change Healthcare for approximately $13 billion.[22]

32. In October 2022, following a Department of Justice antitrust investigation into the merger and a trial ultimately approving the merger, UHG finalized its acquisition of Change Healthcare and integrated it operationally with Optum Insight.[23]

33. As part of the merger, UHG "acquired all of the outstanding common shares of Change Healthcare" and, thus, wholly owns Change Healthcare and is responsible for supervising the cybersecurity practices and protocols of Change Healthcare.[24]

34. At the time of its merger with Change Healthcare in 2022, Optum Insight processed approximately 192 million medical claims annually via its Electronic Data Interchange ("EDI") clearinghouse on behalf of approximately 220 of the approximately 230 health insurance companies in the United States.[25] Via its own EDI clearinghouse network, Optum Insight had the largest collection of claims and electronic medical records

[21] *U.S. v. UnitedHealth Group Inc., and Change Healthcare Inc.*, 1:22-cv-481, Def.'s Proposed Findings of Fact and Conclusions of Law, Dkt. No. 121 at 45 (D.D.C. Sept. 7, 2022).
[22] *U.S. v. UnitedHealth Group Inc., and Change Healthcare Inc.*, 1:22-cv-481, Post-Trial Memorandum Opinion, Dkt. No. 138 at 9 (D.D.C. Sept. 21, 2022).
[23] *U.S. v. UnitedHealth Group Inc., and Change Healthcare Inc.*, 1:22-cv-481, Def.'s Proposed Findings of Fact and Conclusions of Law, Dkt. No. 121 at 11 and 18 (D.D.C. Sept. 7, 2022); James Farrell, *Change Healthcare Blames 'BlackCat' Group for Cyber Attack That Disrupted Pharmacies and Health Systems*, FORBES (Feb. 29, 2024, 1:18 PM),https://www.forbes.com/sites/jamesfarrell/2024/02/29/change-healthcare-blames-blackcat-group-for-cyber-attack-that-disrupted-pharmacies-and-health-systems/ (last visited Jan. 14, 2025).
[24] *Change Healthcare Inc. & UnitedHealth Group Inc*, TAGNIFI, https://viewer.tagnifi.com/deals/TD0000030592 (last visited Jan. 14, 2025).
[25] *U.S. v. UnitedHealth Group Inc., and Change Healthcare Inc.*, 1:22-cv-481, Def.'s Proposed Findings of Fact and Conclusions of Law, Dkt. No. 121 at 19-20 (D.D.C. Sept. 7, 2022).

in the healthcare industry, covering approximately 270 million American lives.[26] The claims data "sent to Optum Insight [] is not de-identified or masked in any way."[27]

35. In support of the merger, UHG and Change Healthcare claimed that the merger would result in significant benefits to the healthcare system, including simplifying and accelerating physician billing and patient payment processes, accelerating cash flow to providers, lowering financial burdens, decreasing the frequency of denied claims, and "minimiz[ing] the amount of friction between payers and providers."[28] The DOJ and the AHA presciently cast doubts on those claims, highlighting the dangers of concentrating essential healthcare services and processes in UHG and Change Healthcare.[29]

III. The Change Platform's Critical Role in the Healthcare Industry

36. Generally, payments for healthcare services in the United States proceed in the following fashion: health insurers like UHIC, also known as "payers," pay medical claims submitted by Providers.[30]

---

[26] *U.S. v. UnitedHealth Group Inc., and Change Healthcare Inc.*, 1:22-cv-481, Def.'s Pretrial Brief, Dkt. No. 103 at 12 (D.D.C. July 22, 2022).

[27] *U.S. v. UnitedHealth Group Inc., and Change Healthcare Inc.*, 1:22-cv-481, Def.'s Proposed Findings of Fact and Conclusions of Law, Dkt. No. 121 at 21 and 26 (D.D.C. Sept. 7, 2022).

[28] *U.S. v. UnitedHealth Group Inc., and Change Healthcare Inc.*, 1:22-cv-481, Post-Trial Memorandum Opinion, Dkt. No. 138 at 9 (D.D.C. Sept. 21, 2022); and *U.S. v. UnitedHealth Group Inc., and Change Healthcare Inc.*, 1:22-cv-481, Def.'s Pretrial Brief, Dkt. No. 103 at 1 (D.D.C. July 22, 2022).

[29] *Testimony of AHA at Hearing "Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack"*, House Committee on Energy and Commerce (Apr. 16, 2024), https://www.aha.org/system/files/media/file/2024/04/24-04-29-AHALTRtoEandConUHG-webwattachment.pdf at 2-3 (last accessed Jan. 14, 2025).

[30] *U.S. v. UnitedHealth Group Inc., and Change Healthcare Inc.*, 1:22-cv-481, Post-Trial Memorandum Opinion, Dkt. No. 138 at 1-2 (D.D.C. Sept. 21, 2022).

37. The process begins with a patient seeking care from a Provider, who confirms insurance coverage (and often collects a co-pay). The Provider then treats the patient or dispenses medication.[31]

38. The Provider then submits a claim to a payer so that the Provider can be compensated for treating the patient.[32]

39. Prior to paying the Provider, the payer evaluates the submitted claim to determine how much, if any, it should pay the Provider for the services rendered.[33]

40. The payer then sends the provider an electronic remittance advice, or ERA, which outlines the claim, and the allowable amounts paid or denied, and pays the Provider the determined amount.[34]

41. The Provider then uses the ERA to bill the patient for any outstanding amounts owed. Alternatively, the Provider may appeal the determination of the payer.

42. The exchanges of information described above occur through EDI clearinghouses, which serve as the "pipes" through which electronic transmission of claims, ERAs, payment remittances, and other information are exchanged between payers and Providers.[35] EDI clearinghouses are used by 95% of Providers and by 99% of insurers.[36]

---

[31] *Id.*
[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] *Id.* at 3-4.
[36] *Id*. at 4.

43. EDI clearinghouse transactions are submitted in standardized transaction formats, which include a substantial amount of highly sensitive patient information in order to effectuate revenue management, clinical decision making, and patient support. [37]

44. In the regular course of business, the Change Health Defendants store massive volumes of highly sensitive and confidential Private Information, including full names, phone numbers, addresses, Social Security numbers, emails, and payment information.

45. The Change Health Defendants also store massive volumes of information protected by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") such as medical records, medical record numbers, dental records, claims information, providers, diagnoses, medicines, test results, images, care and treatment, and billing, claims and payment information (such as claim numbers, account numbers, billing codes, payment cards, financial and banking information, payments made, and balance due). The Change Health Defendants also store massive volumes of health insurance information (such as primary, secondary or other health plans/policies, insurance companies, member/group ID numbers, and Medicaid-Medicare-government payer ID numbers).

46. In theory, the standardized format of information in EDI clearinghouse transactions should enable clearinghouses, Providers, and health insurers to be

[37] *U.S. v. UnitedHealth Group Inc., and Change Healthcare Inc.*, 1:22-cv-481, Def.'s Proposed Findings of Fact and Conclusions of Law, Dkt. No. 121 at 53 and 61 (D.D.C. Sept. 7, 2022); and *U.S. v. UnitedHealth Group Inc., and Change Healthcare Inc.*, 1:22-cv-481, Post-Trial Memorandum Opinion, Dkt. No. 138 at 4 (D.D.C. Sept. 21, 2022).

interoperable across the healthcare industry.[38] In practice, as evidenced by the immense disruption to claims processing following the Ransomware Attack and shutdown, that is not the case. This is partly a function of the fact that Providers connect with the Change Platform either directly or indirectly via a third-party vendor or intermediary.[39] While some Providers contract directly with Change to access the Change Platform, many providers use electronic health records ("EHR") or revenue cycle management ("RCM") vendors to establish an indirect connection to the Change Platform, typically for a monthly flat fee.[40]

47. A further hindrance to Providers simply switching to new EDI clearinghouses is the fact that some payers require the use of a single EDI clearinghouse. Providers and payers are able to transmit claims to clearinghouses for which they do not have a direct or indirect connection via "hops" because EDI clearinghouses have agreements to transmit claims they receive from other EDI clearinghouses on behalf of each EDI's clearinghouse.[41]

48. It is rare for Providers to switch EDI clearinghouses because it is costly and time-intensive to do so. For example, sometimes switching EDI clearinghouses entails switching the entire back-end RCM system into which the EDI clearinghouse integrates.[42]

---

[38] *U.S. v. UnitedHealth Group Inc., and Change Healthcare Inc.*, 1:22-cv-481, Def.'s Proposed Findings of Fact and Conclusions of Law, Dkt. No. 121 at 46 and 52 (D.D.C. Sept. 7, 2022).
[39] *Id.* at 54.
[40] *U.S. v. UnitedHealth Group Inc., and Change Healthcare Inc.*, 1:22-cv-481, Def.'s Proposed Findings of Fact and Conclusions of Law, Dkt. No. 121 at 54 (D.D.C. Sept. 7, 2022); and *U.S. v. UnitedHealth Group Inc., and Change Healthcare Inc.*, 1:22-cv-481, Def.'s Pretrial Brief, Dkt. No. 103 at 10 (D.D.C. July 22, 2022).
[41] *U.S. v. UnitedHealth Group Inc., and Change Healthcare Inc.*, 1:22-cv-481, Def.'s Pretrial Brief, Dkt. No. 103 at 10 (D.D.C. July 22, 2022).
[42] *U.S. v. UnitedHealth Group Inc., and Change Healthcare Inc.*, 1:22-cv-481, Def.'s Proposed Findings of Fact and Conclusions of Law, Dkt. No. 121 at 54 (D.D.C. Sept. 7, 2022).

Even when a full back-end system switch is not necessary, it can take between 60 and 90 days to switch EDI clearinghouses.[43] Indeed, during the 2022 DOJ antitrust trial, evidence from multiple witnesses was presented discussing the profound costs in both time and money to switching EDI clearinghouses and UHG acknowledged that "switching costs are too high" and "[c]auses too much disruption for providers."[44] Two witnesses' testimonies revealed that it could take twelve to eighteen months and over $1 million for a provider to switch from the Change Platform.[45]

49. The ubiquity of the Change Platform is largely a function of its vast network of relationships with payers and Providers.[46] Indeed, as of March 6, 2024, Change had an exclusive payer arrangement with over 1,000 payers in the United States, including in several states, Aetna, BlueCross/Blue Shield, Kaiser, and Medicaid.[47] Such payers only accepted electronic claims through the Change Platform. Including exclusive payers, Change's pervasive network connectivity includes a network of approximately 900,000 physicians, 118,000 dentists, 33,000 pharmacies, 5,500 hospitals, 600 laboratories, and 2,400 government and commercial health insurers.[48]

---

[43] *Id*.
[44] *U.S. v. UnitedHealth Group Inc., and Change Healthcare Inc.*, 1:22-cv-481, DOJ's Proposed Findings of Fact and Conclusions of Law, Dkt. No. 119 at 60 (D.D.C. Sept. 6, 2022).
[45] *Id.* at 61.
[46] *U.S. v. UnitedHealth Group Inc., and Change Healthcare Inc.*, 1:22-cv-481, Def.'s Proposed Findings of Fact and Conclusions of Law, Dkt. No. 121 at 56 (D.D.C. Sept. 7, 2022).
[47] *Exclusive Change Healthcare Payers for Claims*, DrChrono (Mar. 6, 2024), https://support.drchrono.com/home/23548386475163-exclusive-change-healthcare-payers-for-claims-as-of-3-06-2024 (last accessed Jan. 14 2025).
[48] *U.S. v. UnitedHealth Group Inc., and Change Healthcare Inc.*, 1:22-cv-481, Change's Answer to DOJ Complaint, Dkt. No. 38 at 4 and 7 (D.D.C. Mar. 11, 2022).

50. At the time of its merger with Optum Insight, Change operated the country's largest EDI clearinghouse with over half of all commercial medical claims data flowing through the Change Platform.[49] Using its EDI clearinghouse network, Change's Network Solutions business facilitates "'financial, administrative, and clinical transactions, electronic business-to-business and consumer-to-business payments,' as well as aggregation and analytical data services," and generally the transmission of electronic claims.[50] Specifically, the Change Platform processes medical claims relating to 15 billion health care transactions annually, encompassing a third of the patient records in the United States.[51]

51. Change stores and maintains historical claims data flowing through the Change Platform as far back as 2012.[52]

52. Change claims to have "primary" and "secondary" use rights over the data transmitted through its clearinghouse "for purposes beyond providing clearinghouse

[49] *U.S. v. UnitedHealth Group Inc., and Change Healthcare Inc.*, 1:22-cv-481, Post-Trial Memorandum Opinion, Dkt. No. 138 at 8 and 34 (D.D.C. Sept. 21, 2022).
[50] *U.S. v. UnitedHealth Group Inc., and Change Healthcare Inc.*, 1:22-cv-481, Def.'s Proposed Findings of Fact and Conclusions of Law, Dkt. No. 121 at 46 and 52 (D.D.C. Sept. 7, 2022).
[51] *Opening Statement Testimony of Senator Ron Wyden*, Senate Finance Committee (May 1, 2024), https://www.finance.senate.gov/imo/media/doc/0501_wyden_statement.pdf at 1 (last accessed Jan. 14, 2025); and *Opening Statement Testimony of Senator Mike Crapo*, Senate Finance Committee (May 1, 2024), https://www.finance.senate.gov/imo/media/doc/0501_crapo_statement.pdf at 1 (last accessed Jan. 14, 2025).
[52] *U.S. v. UnitedHealth Group Inc., and Change Healthcare Inc.*, 1:22-cv-481, Change's Answer to DOJ Complaint, Dkt. No. 38 at 11 (D.D.C. Mar. 11, 2022).

services" and licenses de-identified data to third parties.[53] In January 2021, Optum Insight estimated that Change had data rights for approximately 90 million Americans annually.[54]

IV. The Ransomware Attack and Shutdown of the Change Platform

53. "Ransomware" is a form of malicious software—or malware—designed to encrypt files on computer devices, rendering any files and the systems that rely on them unusable. After deploying their malware to cripple vulnerable computer systems, malicious actors then demand ransom in exchange for encryption.[55]

54. ALPHV (pronounced "ALF-V") is a well-known Russian-speaking cybercriminal ransomware group that emerged in 2021. ALPHV is also commonly known as BlackCat due to the image of a black cat on its ransomware dark web site.[56]

55. Healthcare Providers and their affiliates like the Change Health Defendants are prime targets for ransomware attacks for two primary reasons. First, they have significant resources to pay ransoms in order to remove encryption and regain control over their networks and systems. Second, the Private Information they collect and store is valuable on black markets.

---

[53] *U.S. v. UnitedHealth Group Inc., and Change Healthcare Inc.*, 1:22-cv-481, Post-Trial Memorandum Opinion, Dkt. No. 138 at 8 (D.D.C. Sept. 21, 2022).
[54] *U.S. v. UnitedHealth Group Inc., and Change Healthcare Inc.*, 1:22-cv-481, Def.'s Proposed Findings of Fact and Conclusions of Law, Dkt. No. 121 at 87 (D.D.C. Sept. 7, 2022).
[55] CYBERSECURITY AND INFRASTRUCTURE AGENCY, *Ransomware Guide* (Sept. 2020), https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf (last visited Jan. 10, 2025).
[56] Christine Barry, *ALPHV-BlackCat ransomware group goes dark*, Barracuda (Mar. 7, 2024), https://blog.barracuda.com/2024/03/06/alphv-BlackCat-ransomware-goes-dark (last viewed Jan. 14, 2025).

56. On February 12, 2024, the username and password for a low-level, customer support employee's access to Change's Citrix portal were posted in a Telegram group chat that advertises the sale of stolen credentials. The account was a basic, user-level account: it only had access to specific applications and did not itself have administrator access or credentials. However, the compromised account had the authority to create accounts with administrative privileges.

57. On February 12, 2024, ALPHV and its affiliates used the compromised credentials to remotely access Change's portal,[57] thus gaining entry to the basic, user-level account.

58. Since "the [Citrix Remote PC Access] portal did not have multi-factor authentication," ALPHV experienced limited roadblocks in gaining access to Change's networks with the compromised credentials.[58]

59. From that limited account, the cybercriminals were able to break into the server that hosted Change's medication management application, SelectRX. This action was undetected by the Change Health Defendants.

60. From there, the cybercriminals created privileged accounts with administrator capabilities that permitted access to and deletion of any and all files, changes to system configurations, and similar administrator-level activities. These actions went to

[57] Testimony of Andrew Witty Chief Executive Officer, UnitedHealth Group Before the House Energy and Commerce Committee Subcommittee on Oversight and Investigations "Examining the Change Healthcare Cyberattack", UnitedHealth Group (May 1, 2024), https://www.congress.gov/118/meeting/house/117242/witnesses/HHRG-118-IF02-Wstate-WittyS-20240501-U5.pdf at 5 (last accessed Jan. 14, 2025).
[58] *Id*.

the heart of the integrity of Change's most critical IT infrastructure, but still went undetected by Change Health Defendants.

61. ALPHV navigated through Change's systems and servers at will, installing multiple malware tools and applications, as well as multiple "backdoors" that would allow the cybercriminals to return to those environments in the event Change detected the suspicious activity and tried to block access.

62. ALPHV also copied and exfiltrated terabytes of Private Information for tens of millions of individuals. ALPHV has disclosed that the data exfiltrated in the Ransomware Attack includes millions of "active U.S. military/navy personnel PII," "medical records," "dental records," "payments information," "claims information," "patients' PII data (i.e., phone numbers, addresses, social security numbers, email addresses, and more," "3000+ source code files for Change Health solutions…," "insurance records," and "more." [59]

63. This access to systems critical to Change's operations went undetected by Change Health Defendants for nine days until the ALPHV chose to reveal itself when it began to encrypt Change's systems on February 21, 2024.

64. On that date, ALPHV ransomware was deployed on Change's networks, "encrypting Change Healthcare's systems" so they could not be accessed without

[59] *Massive Ransomware Attack Disrupts US Healthcare: Behind it, ALPHV/BlackCat*, Heimdal Security (last updated Nov. 19, 2024), available at: https://heimdalsecurity.com/blog/massive-ransomware-attack-disrupts-us-healthcare-behind-it-alphv-blackcat/ (last visited Jan. 14, 2025); Helga Labus, *ALPHV/BlackCat threatens to leak data stolen in Change Healthare cyberattack*, Help Net Security (Feb. 29, 2024), https://www.helpnetsecurity.com/2024/02/29/alphv-blackcat-change-healthcare/ (last accessed Jan. 14, 2025).

ALPHV's cooperation.[60] ALPHV warned Change Health Defendants that they were "walking on a very thin line be careful you just might fall over."[61]

65. Upon learning of the Ransomware Attack, and "[n]ot knowing the entry point of the attack at the time," UHG "immediately severed connectivity with Change's data centers to eliminate the potential for further infection" to "the broader health system."[62]

66. In other words, Change Health Defendants intentionally made the Change Platform inoperable after discovering the Ransomware Attack, severing the connection between Providers and payers.

67. On February 21, 2024, in an SEC filing, UHG announced that "a suspected nation-state associated cyber security threat actor had gained access to some of the Change Healthcare information technology systems."[63] UHG falsely claimed to have "proactively isolated the impacted systems from other connecting systems . . . ."[64] UHG also said it was "working with law enforcement" and allegedly "notified customers, clients and certain

[60] Testimony of Andrew Witty Chief Executive Officer, UnitedHealth Group Before the House Energy and Commerce Committee Subcommittee on Oversight and Investigations "Examining the Change Healthcare Cyberattack", UnitedHealth Group (May 1, 2024), https://www.congress.gov/118/meeting/house/117242/witnesses/HHRG-118-IF02-Wstate-WittyS-20240501-U5.pdf at 4 (last accessed Jan. 14, 2025).

[61] *Notorious ransomware group claims responsibility for attacks roiling US pharmacies*, CyberScoop (Feb. 28, 2024), https://cyberscoop.com/ransomware-alphv-healthcare-pharmacies/ (last viewed Jan. 14, 2025).

[62] Testimony of Andrew Witty Chief Executive Officer, UnitedHealth Group Before the House Energy and Commerce Committee Subcommittee on Oversight and Investigations "Examining the Change Healthcare Cyberattack", UnitedHealth Group (May 1, 2024), https://www.congress.gov/118/meeting/house/117242/witnesses/HHRG-118-IF02-Wstate-WittyS-20240501-U5.pdf at 4 (last accessed Jan. 14, 2025).

[63] *UnitedHealth Group Incorporation Form 8-K*, SEC (Feb. 21, 2024), https://www.sec.gov/Archives/edgar/data/731766/000073176624000045/unh-20240221.htm (last accessed Jan. 14, 2025).

[64] *Id.*

government agencies" of the Ransomware Attack.[65] UHG disclosed that the "network interruption [was] specific to Change Healthcare . . . ."[66] UHG explained it was working to restore Change's information technology systems and resume normal operations as soon as possible but informed the SEC that UHG could not estimate the duration or extent of the disruption at that time.[67]

68. Weeks later, the Change Platform remained largely inoperable.

69. In light of the ongoing shutdown of the Change Platform, on March 13, 2024, the Health and Human Services' Office for Civil Rights ("OCR") sounded the alarm via a Dear Colleague Letter issued to Change wherein OCR emphasized that the Ransomware Attack continued to "pose[] a direct threat to critically needed patient care and essential operations of the health care industry."[68]

70. On April 22, 2024, UHG CEO Andrew Witty reported that files containing Private Information for a substantial proportion of America's population were among the files exfiltrated.[69] Witty further reported that it would take several months of continued analysis before UHG believed it had enough information to begin notifying impacted customers and individuals.[70]

---

[65] *Id.*
[66] *Id.*
[67] *Id.*
[68] *OCR Change Healthcare Dear Colleague Letter*, U.S. DEPT. OF HEALTH AND HUMAN SERVICES (Mar. 13, 2024), https://www.hhs.gov/about/news/2024/03/13/hhs-office-civil-rights-issues-letter-opens-investigation-change-healthcare-cyberattack.html (last visited Jan. 14, 2025).
[69] *UnitedHealth Group Update on Change Healthcare Cyberattack*, UNITEDHEALTH GROUP (Apr. 22, 2024), https://www.unitedhealthgroup.com/newsroom/2024/2024-04-22-uhg-updates-on-change-healthcare-cyberattack.html (last visited Jan. 14, 2025).
[70] *Id.*

71. On April 27, 2024, the AHA provided Congress a letter containing significant information regarding patients' access to care and the financial instability of Providers across the country resulting from the Ransomware Attack.[71] AHA identified "Change Healthcare [as] the predominant source of more than 100 critical functions that keep the health care system operating."[72] According to AHA, Change "processes $2 trillion in health care payments each year," meaning Change is "responsibl[e] for more than 44% of all the dollars flowing through the health care system."[73]

72. As the AHA explained in its letter to Congress, the Ransomware Attack resulted in "patients struggl[ing] to get timely access to care and billions of dollars stopped flowing to providers, thereby threatening the solvency of our nation's provider network."[74] Part of the reason for this was because "[d]uring the early days and weeks of the event, it was very difficult to obtain clear information from UnitedHealth Group. Initially, there was little communication and a minimization from UnitedHealth Group about the impact this event was having on the ability to process medical claims."[75]

73. A third of the hospitals surveyed by AHA reported that the Ransomware Attack "disrupted more than half of their revenue."[76] This figure does not tell the full story

---

[71] *Id.*
[71] *Id.*
[71] *American Hospital Association Letter to Congress*, American Hospital Association (Apr. 29, 2024), https://www.aha.org/system/files/media/file/2024/04/24-04-29-AHALTRtoEandConUHG-webwattachment.pdf at 1 (last accessed Jan. 14, 2025).
[72] *Id.* at 2.
[73] *Id.*
[74] *Id.*
[75] *Id.* at 3.
[76] *Id.*

of the toll on Providers' finances and operations as, post-restoration, Providers still had to "work through the backlog of claims, reprocess denials…, reconcile payments to accounts, and bill patients."[77] Much of this work remains incomplete, even today.

74. On May 1, 2024, Witty testified before both the House Energy and Commerce Committee and the Senate Finance Committee concerning the Ransomware Attack. Witty acknowledged the Ransomware Attack and shutdown "caused incredible disruption across the health care system," resulting in everything from "pharmacists having to manually submit claims to the rural family medicine practice struggling to make payroll."[78] Witty "pledge[d] to do everything in our power to fix [Providers'] system[s] or underwrite their cashflow."[79]

75. Witty also testified about the continued shutdown, acknowledging that UHG was still "mak[ing] substantial progress in restoring Change Healthcare's impacted services" and that a "number of providers [ ] continue to be adversely impacted."[80]

76. Witty confirmed UHG's understanding that "Cyberattacks continue to increase in frequency and significance" and explained that UHG understood the pervasiveness of these attacks, given UHG's own experiences with over 450,000 intrusion attempts annually.[81]

---

[77] *Id.* at 4.
[78] *Opening Statement Testimony of UHG CEO Andrew Witty*, Senate Finance Committee (May 1, 2024), https://www.finance.senate.gov/imo/media/doc/0501_witty_testimony.pdf at 1 (last accessed Jan. 14, 2025).
[79] *Id.* at 5.
[80] *Id.* at 4.
[81] *Id.* at 2.

77. Witty claimed that since Change recently became part of UHG, they "were in the process of upgrading and modernizing their technology" when the Ransomware Attack happened and that "the attack itself had the effect of locking up the various backup systems which had been developed inside Change before it was acquired."[82]

78. Witty also admitted that ALPHV gained access to the Change network because of a lack of MFA on a Change server. More specifically, ALPHV used compromised credentials to infiltrate the network through the externally facing Change server, without MFA restrictions.[83]

79. Witty further estimated one-third of Americans were impacted by the Ransomware Attack.[84] He confirmed that "it is likely to take several months … to identify and notify impacted customers and individuals."[85]

80. Witty confirmed that Private Information from the exfiltrated files had been posted for approximately a week on the dark web and that UHG paid the demanded $22 million ransom in bitcoin.[86]

---

[82] Kapko, Matt, *Change Healthcare Cyberattack: 5 Technical Takeaways from United Health CEO's Testimony*, Cybersecurity Dive (May 6, 2024), https://www.cybersecuritydive.com/news/unitedhealth-change-attack-tech-takeaways/715200/#:~:text=%E2%80%9CThe%20attack%20itself%20had%20the,data%20centers%20before%20the%20attack (last visited Jan. 14, 2025).

[83] *Id.*

[84] Ashley Capoot, *UnitedHealth CEO estimates one-third of Americans could be impacted by Change Healthcare cyberattack*, CNBC (last updated May 20, 2024), https://www.cnbc.com/2024/05/01/unitedhealth-ceo-one-third-of-americans-could-be-impacted-by-change-healthcare-cyberattack.html (last visited Jan. 14, 2025).

[85] *Opening Statement Testimony of UHG CEO Andrew Witty*, Senate Finance Committee (May 1, 2024), https://www.finance.senate.gov/imo/media/doc/0501_witty_testimony.pdf at 3 (last accessed Jan. 14, 2025).

[86] *Witty Response to Questions for the Record*, Senate Finance Committee (May 1, 2024),

81. However, after ALPHV received UHG's ransom payment, it chose not to share the ransom with its affiliate who executed the attack, known as "notchy," and instead, "published a fake law enforcement takedown notice on their leak site before disappearing with the full $22 million."[87]

82. Notchy confirmed that, because it was not paid its share of the ransom by ALPHV, it would retain the stolen data, stating: "Sadly for Change Healthcare, their data [is] still with us."[88]

83. Notchy and other former ALPHV affiliated groups have since joined the ransomware group RansomHub.[89]

84. RansomHub has since confirmed that it possesses 4 terabytes of the Change Health Defendants' stolen data by posting screenshots on its dark web ransomware site and has attempted to extort Change Health Defendants out of additional ransom payments.[90]

85. In response to ALPHV refusing to pay notchy, Dmitry Smilyanets, a researcher for the security firm Recorded Future, said, "[t]he affiliates still have this data,

---

https://www.finance.senate.gov/imo/media/doc/responses_for_questions_for_the_record_to_andrew_witty.pdf at 5 and 40 (last accessed January 14, 2025).

[87] *RansomHub Has Change Healthcare Data – BlackCat/ALPHV Rebrand?*, Halcyon (Apr. 15, 2024), https://www.halcyon.ai/attacks-news/ransomhub-has-change-healthcare-data---BlackCat-alphv-rebrand (last visited Jan. 14, 2025).

[88] *BlackCat Ransomware Group Implodes After Apparent $22M Payment by Change Healthcare*, Krebs on Security (Mar. 5, 2024), https://krebsonsecurity.com/2024/03/BlackCat-ransomware-group-implodes-after-apparent-22m-ransom-payment-by-change-healthcare/ (last visited Jan. 14, 2025).

[89] Christine Barry, *Change Healthcare and RansomHub redefine double extortion*, Barracuda (Apr. 12, 2024), https://blog.barracuda.com/2024/04/12/change-healthcare-and-ransomhub-redefine-double-extortion (last visited Jn. 14, 2025).

[90] Ionut Arghire, *Ransomware Group Starts Leaking Data Allegedly Stolen From Change Healthcare*, Security Week (Apr. 16, 2024), https://www.securityweek.com/ransomware-group-starts-leaking-data-allegedly-stolen-from-change-healthcare/ (last visited Jan. 14, 2025).

and they're mad they didn't receive this money. . . . It's a good lesson for everyone. You cannot trust criminals; their word is worth nothing."[91]

86. The number of individuals in the United States that have been affected by the Ransomware Attack is astounding. On October 22, 2024, Change notified OCR that it had already sent individual notices to approximately 100 million Americans.[92]

87. As for the continued shutdown of the Change Platform, Services slowly began to resume at partial levels for some users beginning in late March and April 2024.

88. However, it was not until November 21, 2024, *nine months* after the initial shutdown, that Change reported that it had purportedly "complete[d] restoration of its clearinghouse services."[93] Even then, Change was only offering "partial service" for some Services.

V. The Aftermath of the Ransomware Attack for Providers

89. The Change Health Defendants' decision to shut down the Change Platform without warning to the Providers and insurers that were dependent on the Platform and without offering an adequate substitute wreaked chaos throughout the healthcare system

[91] *BlackCat Ransomware Group Implodes After Apparent $22M Payment by Change Healthcare*, Krebs on Security (Mar. 5, 2024), https://krebsonsecurity.com/2024/03/BlackCat-ransomware-group-implodes-after-apparent-22m-ransom-payment-by-change-healthcare/ (last visited Jan. 14, 2025).

[92] *OCR Change Healthcare Cybersecurity Incident Frequently Asked Questions*, U.S DEPT. OF HEALTH AND HUMAN SERVICES (Oct. 24, 2024), https://www.hhs.gov/hipaa/for-professionals/special-topics/change-healthcare-cybersecurity-incident-frequently-asked-questions/index.html (last visited Jan. 14, 2025).

[93] *Change Healthcare's Clearinghouse Services Available Now After the February Ransomware Attack*, Compliance Home (Nov. 22, 2024) https://www.compliancehome.com/change-healthcares-clearinghouse-services-available-now-after-the-february-ransomware-attack/ (last visited Jan. 14, 2025).

which, as a result of Defendants' mergers and expansion throughout the industry, was dependent on the Change Platform as essential infrastructure for the provision of patient care.

90. The Change Health Defendants' decision acutely impacted Providers by cutting off their ability to submit insurance claims and receive payment. Other Services that Providers relied on were also cut off, such as their ability to receive ERAs and conduct patient eligibility checks.

91. Change Health Defendants were unable to fully restore these Services for months after the Ransomware Attack, and some Providers are still unable to access ERAs.

92. By cutting off Providers from necessary healthcare system infrastructure and substantial cash inflows for months, the Ransomware Attack and resulting shutdown decimated healthcare practices nationwide.

93. Change Health Defendants' decision to shut down the Change Platform caused Providers to experience loss or delay of months' worth of income, and forced Providers to divert resources from their ordinary operations, including patient care.

94. Change Health Defendants' decision to publish incomplete and misleading information regarding the duration and extent of the shutdown exacerbated these injuries.

a. The Ransomware Attack and shutdown interfered with Providers' services caused Providers to experience losses or delays of substantial income.

95. The Change Platform outage impacted Providers' ability to provide their services and to obtain compensation for the services they were able to provide to patients in numerous ways.

96. When Change Health Defendants disconnected the Change Platform, many Providers lost their primary (and, in some cases, their only) method for processing insurance claims for their services, including both private insurance and government-provided healthcare plans such as Medicare. Because these Providers could not submit and/or have their claims processed for months, they did not receive payment from insurance companies or the government for months. For example, a survey conducted by the American Medical Association (AMA) two months after the Ransomware Attack revealed that 80% of responding physician practices were still losing revenue from the inability to submit claims.[94]

97. Some Providers resorted to submitting paper claims through the mail, a laborious process that required enormous human resources on the part of Providers. Providers either had to marshal additional human resources to undertake paper claims submissions, or were simply unable to submit claims. Two months after the Ransomware Attack, the AMA survey revealed that 91% of surveyed physician practices still had to commit additional staff time and resources to complete revenue cycle tasks.[95] Many insurers became so overrun by paper claims during the outage that they encouraged Providers to stop submitting paper claims due to long delays processing paper claims. These delays further delayed payment to Providers or prevented payment altogether.

[94] *Change Healthcare cyberattack impact*, AM. MED. ASS'N, at 2 (April 29, 2024), https://www.ama-assn.org/system/files/change-healthcare-follow-up-survey-results.pdf (last accessed Jan. 14, 2025).
[95] *Id.*

98. Providers also exerted resources by trying to switch clearinghouses so they could submit claims through those alternative services. However, attempting to switch clearinghouses on an expedited timeline created costs associated with switching, increases in rejected claims, interoperability issues with some insurers, and lost employee time implementing and learning a new system.

99. Switching clearinghouses was also not a panacea. Many insurers accepted electronic claims *exclusively* through the Change Platform. When Change Health Defendants shut down the Change Platform, Providers—regardless of whether they exclusively used the Change Platform—could only submit claims to those insurers by paper and mail. Switching to another clearinghouse was simply not an option because these payers did not work with any clearinghouses other than Change.

100. As a result of Change Health Defendants' decision to take the Change Platform offline, Providers were (and some still are) unable to receive ERAs for claims that were (i) submitted via the Change Platform shortly before the shutdown, and (ii) claims that were submitted via alternate routes (such as by paper or through an alternative clearinghouse) during the shutdown. Without ERAs, Providers have no way of knowing which claims insurers have accepted, partially accepted, or rejected, and are unable to go through the normal process of addressing these issues to ensure that they receive full payment before insurers' Timely Filing Deadlines.[96]

[96] Insurers require Providers to submit and resolve claims within a certain number of days of providing service to the patient. These deadlines are referred to as "Timely Filing Deadlines." Claims submitted or resolved after the Timely Filing Deadline, are not paid by the insurer.

101. Providers were unable to engage in payment reconciliations and decide which denials to appeal without ERAs. As a result, Providers missed out on payments, entirely or partially, on claims for which they never received ERAs or for which they received delayed ERAs.

102. Two months after the Ransomware Attack and shutdown, 79% of surveyed physician practices were still unable to receive ERAs.[97] Some Providers remain unable to receive or access historical ERAs.

103. In addition to being unable to perform reconciliations by using the ERAs, due to the length of the shutdown, there are some claims for which Providers were unable to make *any submission* by the Timely Filing Deadlines. With no or limited ability to submit claims, the Ransomware Attack and subsequent Change Platform shutdown caused many Providers to have claims denied by insurers for not complying with the Timely Filing Deadlines. Providers will never be paid for these claims because of Change Health Defendants' shutdown.

104. Just two months after the Ransomware Attack and shutdown, 27% of surveyed physician practices reported that they had already had claims denied for failing to meet Timely Filing Deadlines because of the Ransomware Attack and shutdown.[98]

105. Moreover, as a result of Change Health Defendants' shutdown of the Change Platform, Providers were unable to check patient coverage or eligibility for prescriptions and services. In some cases, Providers had to delay services or turn patients away, including

[97] *Id.* at 1.
[98] *Id.* at 3.

for new patients whose insurance coverage Providers could not verify due to the shutdown. In other cases, patients were unwilling to proceed with treatment not knowing how much of the prescription or service was going to be covered by the insurer. Similarly, some patients were unable to get timely prior authorizations for needed care, further depriving Providers of income.[99]

106. Providers had to absorb these costs and losses in real time, impacting not only their financial stability but in many instances, their ability to provide patient care. Providers took lines of credit from banks and used their personal savings to afford employee payroll, rent, and other expenses, and they racked up duplicated payment software charges. To persevere through the shutdown, some Providers cut resources for patients by, for example, reducing the amount of supplies on hand. The administrative and financial challenges created by the Change shutdown forced at least 91% of respondents to the AMA survey to divert staff time and resources to administrative tasks, and caused many Providers to delay or forgo seeing patients.[100]

107. The loss of substantial income to Providers came at a time when interest rates were at recent highs. The AMA survey revealed that, two months after the Ransomware Attack and shutdown, 62% of surveyed physician practices were still using personal funds

[99] *Massive cyberattack crippled a healthcare payment system a month ago. It's not fixed yet.*, NJ.COM (Mar. 20, 2024), https://www.nj.com/news/2024/03/massive-cyberattack-crippled-a-healthcare-payment-system-a-month-ago-its-not-fixed-yet.html (last visited Jan. 14, 2025).

[100] *Change Healthcare cyberattack impact*, AM. MED. ASS'N, at 2 (April 29, 2024), https://www.ama-assn.org/system/files/change-healthcare-follow-up-survey-results.pdf (last accessed Jan. 14, 2025).

to cover practice expenses while 29% had taken out private bank loans.[101] One survey respondent stated that "Having to borrow from my bank at 14% interest is a hardship I will never recoup."[102] Many Providers are still paying down loans that they were required to take out during the outage to keep their doors open to patients in need, to the extent they could do so, and continue paying their staff.

b. Change Health Defendants' misleading statements and omissions during the shutdown caused further damage.

108. To make matters worse, throughout the shutdown Change Health Defendants published misleading statements and omitted key facts regarding the impact of the Ransomware Attack. These statements were intended to (and did) deceive Providers into believing that the Change Platform would be back online quickly and to hide Change Health Defendants' ineptitude from the public.

109. In reality, Change Health Defendants had exclusive knowledge of facts that clearly indicated it would be months before the Change Platform was up and running at its previous capacity. These facts, which only Change Health Defendants were privy to, included (i) the extensive damage caused by the cybercriminals, (ii) Change Health Defendants' lack of disaster recovery or business continuity plans and preparations to provide an adequate substitute for the Services offered on the Change Platform, and (iii) the labor required to reconnect the massive volume of entities to the Change Platform, all of which are required for the Platform to function at full capacity.

[101] *Id.* at 2.
[102] *Id.*

110. Despite this knowledge, Change Health Defendants persisted in making several misleading statements and omitting key facts that would have allowed Providers to mitigate their damages.

111. For example, when Change Health Defendants disclosed the Change Platform was the subject of the Ransomware Attack on February 21, 2024, they optimistically stated that they were "working diligently to restore those systems and resume normal operations as soon as possible, but cannot estimate the duration or extent of the disruption at this time."[103] In reality, Change Health Defendants knew it would take months—not days or weeks—to restore the Change Platform.

112. On each day between February 21 and February 28, 2024, Optum, Inc. provided an update regarding the shutdown, again emphasizing that the Change Health Defendants were working to restore Services:[104]

> We are working on multiple approaches to restore the impacted environment and will not take any shortcuts or take any additional risk as we bring our systems back online. We will continue to be proactive and aggressive with all our systems and if we suspect any issue with the system, we will immediately take action and disconnect. ***The disruption is expected to last at least through the day.***

113. Discovery will show that sometime between February 21 and February 28, 2024, Change Health Defendants came to understand the shutdown would last much longer

---

[103] *UnitedHealth Group Incorporation Form 8-K*, SEC (Feb. 21, 2024), https://www.sec.gov/Archives/edgar/data/731766/000073176624000045/unh-20240221.htm (last visited Jan. 14, 2025).

[104] *Update: restoration in progress of Change Healthcare products and services*, Optum (Feb. 21, 2024 to Feb. 28, 2024), https://solution-status.optum.com/incidents/hqpjz25fn3n7 (emphasis added) (last visited Jan. 14, 2025).

than a day, or even weeks. Despite this knowledge, Change Health Defendants failed to remove the misleading statement on the Optum website stating the "disruption is expected to last at least through the day," and omitted a truthful assessment of how long the shutdown would last.

114. On February 29, 2024, UHG COO Dirk McMahon said that UHG was setting up a loan program to help Providers who could not submit insurance claims while Change is offline. He stated the program would last "for the ***next couple of weeks*** as this continues to go on."[105]

115. Discovery will show that as of February 29, Change Health Defendants knew that the Change Platform would not be fully operational for much longer than a couple weeks. Despite this knowledge, Change Health Defendants misleadingly stated the Change Platform would be offline for a "couple of weeks" and omitted that even when the Change Platform came back online, it would not be fully operational, and that several Services would not be available at all.

116. On March 7, 2024, UHG published a press release addressing the "Timeline to Restore Change Healthcare Systems."[106] The press release stated that "[a]ssuming we continue at our current rate of progress, we expect our key system functionality to be restored and available on the following timelines: . . . Medical claims: We expect to begin

[105] *UnitedHealth Says 'BlackCat' Ransomware Group Behind Hack at Tech Unit*, Reuters (Feb. 29, 2024), https://www.reuters.com/technology/unitedhealth-confirms-blackcat-group-behind-recent-cyber-security-attack-2024-02-29/ (last visited Jan. 14, 2025) (emphasis added).

[106] Press Release, UnitedHealth Group, *UnitedHealth Group Update on Change Healthcare Cyberattack* (Mar. 7, 2024), https://www.unitedhealthgroup.com/newsroom/2024/2024-03-07-uhg-update-change-healthcare-cyberattack.html (last visited Jan. 14, 2025).

testing and reestablish connectivity to our claims network and software ***on March 18, restoring service through that week***."[107] UHG claimed that all major pharmacy claims and payment systems were back up and functioning and that UHG had taken action to make sure patients could access their medicines.[108]

117. Discovery will show that as of March 7, Change Health Defendants knew that many users of the Change Platform, including both insurers and providers, would not have "key system functionality" restored by the week of March 18. Despite this knowledge, Change Health Defendants misleadingly stated the Change Platform would be restored on March 18 and the following week, omitted that it would take much longer to get all users of the platform reconnected, and omitted that even when the Change Platform came back online, it would not be fully operational and several Services would not be available at all. Change Health Defendants further failed to later update and correct these misleading statements regarding medical claims functionality despite having a duty to do so after choosing to make statements on the topic.

118. Change Health Defendants' statements regarding pharmacies were also false. In his May 1, 2024, testimony before both the House Energy and Commerce Committee and the Senate Finance Committee, Witty acknowledged that it was not until late April 2024 that pharmacy claims Services had been restored to near full pre-breach levels and that some pharmacies still had not had their capacity to utilize claims Services restored.[109]

---

[107] *Id.* (emphasis added)
[108] *Id.*
[109] *Witty Response to Questions for the Record*, Senate Finance Committee (May 1, 2024),

119. Also on April 22, 2024, two months after the Ransomware Attack, Change Health Defendants stated in a press release that "[m]edical claims across the U.S. health system are now flowing at near-normal levels as systems come back online ***or providers switch to other methods of submission***. Change Healthcare realizes there are a small number of providers who continue to be adversely impacted."[110] Change Health Defendants further admitted payment processing was still only at "86% of pre-incident levels," and other Services, such as eligibility software, were still in the process of "being restored on a rolling basis."[111]

120. Change Health Defendants' April 22, 2024 statements were false and misleading, and omitted critical facts, as to the true state of the Change Platform.

121. For example, on April 29, 2024, the AMA released the results of a survey of physician practices on the continuing impacts of the Ransomware Attack and shutdown taken between April 19 and April 24, 2024.[112] The survey revealed that 60% continued to face challenges in verifying patient eligibility; 75% still faced barriers with claim submission; 79% still could not receive ERAs; and 85% continued to experience disruptions in claim payments.[113]

---

https://www.finance.senate.gov/imo/media/doc/responses_for_questions_for_the_record_to_andrew_witty.pdf at 28 (last accessed Jan. 14, 2025).

[110] *UnitedHealth Group Updates on Change Healthcare Cyberattack*, UnitedHealth Group (Apr. 22, 2024), https://www.unitedhealthgroup.com/newsroom/2024/2024-04-22-uhg-updates-on-change-healthcare-cyberattack.html (last accessed Jan. 14, 2025) (emphasis added).

[111] *Id.*

[112] *Change Healthcare cyberattack impact*, AM. MED. ASS'N, at 1 (April 29, 2024), https://www.ama-assn.org/system/files/change-healthcare-follow-up-survey-results.pdf (last accessed Jan. 14, 2025).

[113] *Id.* at 1.

122. The AMA survey responses indicated the additional harm Change Health Defendants' misleading statements and omission had on Providers, with one survey respondent stating:

> We are still not able to send electronic claims, yet Medicare and other insurances are saying to bill electronically because Change is back online, when the platform we use will not be online for months.[114]

This statement indicates that insures and government payers relied on Change Health Defendants' false and misleading statements and omissions regarding the restoration of the Change Platform to Providers' detriment.

123. The AMA survey responses also revealed that 84% of surveyed physician practices "indicated that they are not receiving information, or are receiving inaccurate information, regarding service restoration from [Change Health Defendants]."[115]

124. The continued adverse impact is reflected in online forums created by Providers to try to help and support each other following the Ransomware Attack. For example, in a June 6, 2024, Reddit post titled "Change/Optum healthcare claims processing STILL down" various Providers discussed the reality that claims processing continued "to be down for three plus months for multiple practices throughout the country. No end in sight."[116]

---

[114] *Id.*
[115] *Id.* at 2.
[116] *Change/Optum healthcare claims processing STILL down*, Reddit (June 6, 2024), https://www.reddit.com/r/CodingandBilling/comments/1da0em9/changeoptum_healthcare_claims_processing_still/ (last visited Jan. 14, 2025).

125. Publicly available facts show the restoration was still not complete nearly six months after the Ransomware Attack and shutdown. For example, on August 8, 2024, Blue Cross Blue Shield of Massachusetts stated that it reconnected to Change Platform for some, but not all, functionality. Specifically, it reported it had restored connectivity to the Change clearinghouse but was still working to process ERAs that had been held during the shutdown.[117]

126. Moreover, on or around November 21, 2024, nine months after the Ransomware Attack and shutdown, Change reported it had purportedly "complete[d] restoration of its clearinghouse services."[118] Even then, Change was only offering "partial service" for some Services.

127. Even today, Providers who changed to new clearinghouses are unable to access ERAs from Change.

128. Change Health Defendants' misleading statements and omissions, which were widely covered in the media and reported to and relied on by Providers, prevented

[117] *Change Healthcare Event*, Provider Center, Blue Cross Blue Shield of Massachusetts (last updated Aug. 8, 2024), https://provider.bluecrossma.com/ProviderHome/portal/home/ChangeHealthcareEvent/!ut/p/z1/lZBNC4JAEIZ_jdedcU3dumkHSw0jEG0voWJqqCtq-vezTgnSxzCXged5YV7gEAKvo6HIor4QdVRO95lrlx3db2WHoWcxT0Ht4DLdto_UclQIXgDOxkDzRE0F0fIo8P_996Tf_A8A_xwfAF9A5h98y7CBF3FFxqQiSDR9xWRGp12jRlXlWaFRxwrLgLfpNW3Tltzbqdm875tuI6GE4ziSTIisTEkiKgmXlFx0PYRzEprK90O8qeXgGg9eKXnH/dz/d5/L2dBISEvZ0FBIS9nQSEh/?ICID=chc_outage (last visited Jan. 14, 2025).

[118] Thomas Brown, *Change Healthcare's Clearinghouse Services Available Now After the February Ransomware Attack*, Compliance Home (Nov. 22, 2024) https://www.compliancehome.com/change-healthcares-clearinghouse-services-available-now-after-the-february-ransomware-attack/#:~:text=Change%20Healthcare%20has%20reported%20the,of%20Amedisys%20by%20UnitedHealth%20Group (last accessed Jan. 14, 2025).

Providers, insurers, and EHR vendors from making informed decisions during the shutdown. For example, had Change Health Defendants disseminated accurate and complete information about how long it would take to restore the functionality of the Change Platform, Providers could have made informed decisions about obtaining financing, investing the resources to switch to alternative clearinghouses, obtaining resources to submit paper claims, negotiating Timely Filing Deadlines, obtaining alternative financing, and keeping employees on payroll.

129. The full impact of the Ransomware Attack on Providers is enormous and not yet fully known, and its effects are currently being felt by Providers nationwide.

c. UHG financially benefitted from the Ransomware Attack and shutdown.

130. Amidst all the harm Change Health Defendants' conduct inflicted upon the healthcare system and Providers specifically, UHG acknowledged that it experienced certain *positive* financial impacts resulting from the Ransomware Attack.

131. For example, on April 16, 2024, UHG reported that the business disruptions caused by the Ransomware Attack had a positive $48 million tax effect, with an estimated benefit of $70 to $90 million in year-end impact.[119] UHG estimated the total tax effect of the Ransomware Attack was $189 million for the first quarter with a $305 million to $375 million total tax effect by year end.[120]

[119] *UnitedHealth Group Inc. First Quarter 2024 Results*, UnitedHealth Group (Apr. 16, 2024), https://www.unitedhealthgroup.com/content/dam/UHG/PDF/investors/2024/UNH-Q1-2024-Release.pdf at 19 (last accessed Jan. 14, 2025).
[120] *Id.*

132. On July 16, 2024, UHG reported the total estimated tax effect of the Ransomware Attack was $252 million for the second quarter with an estimated $515 million to $560 million total tax effect by year end.[121] UHG estimated the total tax effect of the direct response as a result of the Data Breach was $182 million for the second quarter and $323 million for the first two quarters combined.[122]

133. These positive tax benefits comport with UHG's representations to the SEC that "the Company has not determined the incident is reasonably likely to materially impact the Company's financial condition…."[123]

134. Much of the positive financial impact of the Ransomware Attack and shutdown for UHG is attributable to UHIC, UHG's health insurance company. During the shutdown, UHIC, like many other insurers, did not experience a dip in income because members were still paying premiums. UHIC and other insurers, however, were not paying Providers for the medical services members received during the shutdown because Providers were unable to submit claims. Instead of paying out that money owed to Providers, UHIC and other insurers held those millions (if not billions) of dollars in their cash reserves, earning interest at a time when interest rates were at recent highs.

---

[121] *UnitedHealth Group Inc. Second Quarter 2024 Results*, UnitedHealth Group (Jul. 16, 2024), https://www.unitedhealthgroup.com/content/dam/UHG/PDF/investors/2024/UNH-Q2-2024-Release.pdf at 16 (last accessed Jan. 14, 2025).

[122] *Id.* at 17.

[123] UnitedHealth Group Incorporated, Form 8-K (Feb. 21, 2024), available at https://www.sec.gov/Archives/edgar/data/731766/000073176624000045/unh-20240221.htm (last accessed Jan. 14, 2025).

135. Moreover, UHIC has aggressively enforced Timely Filing Deadlines for claims that could not be submitted because of the shutdown, permanently denying payment to struggling Providers while enriching UHG.

d. Defendants' Temporary Funding Assistance Program was inadequate, and Defendants are prematurely demanding providers repay the loans.

136. Following the shutdown, Defendants established the TFAP loan program administered by the Optum Financial Defendants to provide interest-free and fee-free loans to eligible Providers affected by the Ransomware Attack and shutdown, which Providers would then repay once they recovered from the financial strain imposed by the shutdown.

137. TFAP was launched on March 1, 2024, following Congressional hearings and criticism of Change Health Defendants' response to the Ransomware Attack and shutdown.

138. Providers could submit an inquiry form within an online portal created for TFAP, and, if deemed eligible, they could then log into their Optum Pay account to view their organization's funding amount and from there request and accept the funds that would be deposited to the bank account on file in Optum Pay.

139. The Provider would then receive TFAP funds in weekly allotments, if it so requested.

140. The Optum Pay online portal allowed Providers to view past loan payments and repayment status, and to submit repayments.

141. At first Providers were offered small loans that did not come close to bridging the gap in payments left in the wake of the shutdown. However, Defendants later increased

the loan amounts available to Providers and many Providers utilized the Program to help offset the amounts in funding they would have to obtain from other sources in order to remain afloat during the prolonged shutdown.

142. At the May 1, 2024, Congressional Hearing, Witty discussed UHG's TFAP, explaining that Providers had 45 business days following the resumption of claims processing to repay any zero interest loans advanced to Providers as a result of the Ransomware Attack.[124] Witty confirmed that UHG had "no intention of asking for repayment until providers determine their business is back to normal."[125]

143. The TFAP Agreements were made between Providers and Change Healthcare Operations, LLC. As updated on March 15, 2024, under section 5(a), the Agreement states:

> Recipient agrees to pay the total Funding Amount disbursed to Recipient in full within forty-five (45) business days of receiving notice that the Funding Amount is due ("Repayment Date"). CHC will send notice to the Recipient that the Funding Amount is due after claims processing and or/payment processing services have resumed and payments impacted during the service disruption period are being processed. In the event of a failure to repay CHC the full Funding Amount due on the Repayment Date, CHC may seek repayment as outlined in Section 5(b).

[124] *Responses to Questions for the Record for Andrew Witty*, U.S. Senate Committee on Finance, Full Committee Hearing, at 14 (May 1, 2024), available at https://www.finance.senate.gov/imo/media/doc/responses_for_questions_for_the_record_to_andrew_witty.pdf (last accessed Jan. 14, 2025).
[125] *Id.* at 34.

144. Despite this agreement, Defendants have demanded repayment before payments impacted during the service disruption period have been processed and claims deemed untimely may never be paid or processed.

145. As of October 24, 2024, the Optum Financial Defendants had disbursed $8.9 billion in loans to Providers through the TFAP and had recovered $3.2 billion in repayments.

VI. Change Health Defendants Are Responsible for the Ransomware Attack and Shutdown

a. Change Health Defendants knew of the acute risk of ransomware attacks for businesses in the healthcare industry.

146. Change Health Defendants' data security obligations were particularly important given the substantial increase in Ransomware Attacks targeting healthcare entities that collect and store Private Information preceding the date of the Attack.

147. The increased risk to healthcare entities was known and obvious to Change Health Defendants as they observed frequent public announcements of ransomware attacks affecting healthcare providers and knew that information of the type they collect, maintain, and store is highly coveted and a frequent target of cybercriminals.

148. There have been recent high profile cybersecurity incidents at other healthcare partner and provider companies, including ESO Solutions, Inc. (2.7 million patients, September 2023), HCA Healthcare (11 million patients, July 2023), HealthEC LLC (4 million patients, July 2023), Prospect Medical Holdings, Inc. (1.3 million patients, July-August 2023), Managed Care of North America (8 million patients, March 2023), PharMerica Corporation (5 million patients, March 2023), Florida Orthopedic Institute

(640,000 patients, July 2020), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), BJC Health System (286,876 patients, March 2020), American Medical Collection Agency (25 million patients, March 2019), Oregon Department of Human Services (645,000 patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), and Wolverine Solutions Group (600,000 patients, September 2018).

149. According to the HIPAA Journal's 2023 Healthcare Ransomware Attack Report, "[a]n unwanted record was set in 2023 with 725 large security breaches in healthcare reported to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR), beating the record of 720 healthcare security breaches set the previous year."[126]

150. In addition, the Identity Theft Resource Center ("ITRC") set a new record for the number of data compromises tracked in a year, up 72% from the previous all-time high in 2021 (1,860).[127]

151. Further, in Change Healthcare's 2022 Form 10-K disclosures, it acknowledged the broad range of risks that are attributed to its field of business and its own company specifically. Change Healthcare claimed that:

[126] Steve Adler, *Security Breaches in Healthcare in 2023*, The HIPAA Journal (Jan. 31, 2024), https://www.hipaajournal.com/wp-content/uploads/2024/01/Security_Breaches_In_Healthcare_in_2023_by_The_HIPAA_Journal.pdf (last accessed Jan. 14, 2025).

[127] *ITRC Data Breach Report 2023*, ITRC (2023), https://www.idtheftcenter.org/publication/2023-data-breach-report/ (last accessed Jan. 14, 2025).

a. Its Services "involve the use and disclosure of personal and business information that could be used to impersonate third parties or otherwise gain access to their data or funds. If any of our employees or vendors or other bad actors takes, converts, or misuses such funds, documents or information, or we experience a data breach creating a risk of identity theft, we could be liable for damages, and our reputation could be damaged or destroyed;"[128]

b. It could "be perceived to have facilitated or participated in illegal misappropriation of funds, documents or data and, therefore, be subject to civil or criminal liability. Federal and state regulators may take the position that a data breach or misdirection of data constitutes an unfair or deceptive act or trade practice;"[129]

c. "Despite [its] security management efforts […] [its] infrastructure, data or other operation centers and systems used in connection with [its] business operations, including the internet and related systems of [its] vendors . . . are vulnerable to, and may experience, unauthorized access to data and/or breaches of confidential information due to criminal conduct;"[130] and

d. "[Its] products and services involve processing personal information. Like many organizations, [the UHG companies] have been and expect to routinely

[128] Change Healthcare, 2022 Form 10-K (May 26, 2022), available at https://www.sec.gov/Archives/edgar/data/1756497/000175649722000007/chng-20220331x10k.htm (last accessed Jan. 14, 2025).
[129] *Id*.
[130] *Id*.

be the target of attempted cyber and other security threats by outside third parties, including technologically sophisticated and well-resourced bad actors attempting to access or steal the data [they] store."[131]

152. In UHG's SEC Form 10-K disclosures for the fiscal year ended December 31, 2023, which also analyzed and disclosed risks associated with Optum Insight, UHG and Optum Insight recognized that:[132]

a. "If we or third parties we rely on sustain cyber-attacks or other privacy or data security incidents resulting in disruption to our operations or the disclosure of protected personal information or proprietary or confidential information, we could suffer a loss of revenue and increased costs, negative operational affects, exposure to significant liability, reputational harm and other serious negative consequences."

b. "We are regularly the target of attempted cyber-attacks and other security threats and have previously been, and may in the future be, subject to compromises of the information technology systems we use, information we hold, or information held on our behalf by third parties."

c. "Threat actors and hackers have previously been, and may in the future be, able to negatively affect our operations by penetrating our security controls and causing system and operational disruptions or shutdowns, accessing,

[131] *Id*.

[132] UnitedHealth Group Incorporated, 2023 Form 10-K (Feb. 28, 2024), available at https://www.unitedhealthgroup.com/content/dam/UHG/PDF/investors/2023/UNH-Q4-2023-Form-10-K.pdf (last accessed Jan. 14, 2025).

misappropriating or otherwise compromising protected personal information or proprietary or confidential information or that of third parties, and developing and deploying viruses, ransomware and other malware that can attack our systems, exploit any security vulnerabilities, and disrupt or shutdown our systems and operations."

d. "There have previously been and may be in the future heightened vulnerabilities due to the lack of physical supervision and on-site infrastructure for remote workforce operations and for recently-acquired or non-integrated businesses. We rely in some circumstances on third-party vendors to process, store and transmit large amounts of data for our business whose operations are subject to similar risks."

e. "[C]ompromises of our security measures or the unauthorized dissemination of sensitive personal information, proprietary information or confidential information about us, our customers or other third parties, previously and in the future, could expose us or them to the risk of financial or medical identity theft, negative operational affects, expose us or them to a risk of loss or misuse of this information, result in litigation and liability, including regulatory penalties, for us, damage our brand and reputation, or otherwise harm our business."

153. Moreover, prior to the Ransomware Attack, government agencies and cybersecurity researchers provided repeated warnings to healthcare entities of the threat posed by ALPHV.

b. Change Health Defendants had duties to protect Private Information.

154. Change Health Defendants are covered by HIPAA (*see* 45 C.F.R. § 160.102) and, as such, are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

155. These rules establish national standards for the protection of patient information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. 45 C.F.R. § 160.103.

156. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."[133]

157. HIPAA requires that Change Health Defendants implement appropriate safeguards for this information.[134]

158. HIPAA requires that covered entities provide notice of a breach of "unsecured" protected health information. "Unsecured" protected health information

[133] 45 C.F.R. § 164.502.
[134] 45 C.F.R. § 164.530(c)(1).

means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons—i.e., non-encrypted data.[135]

159. In addition to HIPAA, federal agencies have issued recommendations and guidelines to help minimize the risks of a ransomware attack for businesses holding Private Information. For example, the Federal Trade Commission (FTC) has issued numerous guides for businesses highlighting the importance of reasonable data security practices, which should be factored into all business-related decision making.[136]

160. The FTC's publication Protecting Personal Information: A Guide for Business sets forth fundamental data security principles and practices for businesses to implement and follow as a means to protect sensitive data.[137] Among other things, the guidelines state that businesses should (a) protect the personal customer information that they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network's vulnerabilities; and (e) implement policies to correct security problems. The FTC guidelines further recommend that businesses use an intrusion detection system, monitor all incoming traffic for unusual activity, monitor for large amounts of data being transmitted from their system, and have a response plan ready in the event of a breach.[138]

---

[135] 45 C.F.R. § 164.404; 45 C.F.R. § 164.402.

[136] *Start with Security*, FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed Jan. 14, 2025).

[137] *Protecting Personal Information, A Guide for Business*, FTC, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Jan. 14, 2025).

[138] *Id*.

161. Additionally, the FTC recommends that companies limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[139] This is consistent with guidance provided by the FBI, HHS, and the principles set forth in the Cybersecurity and Infrastructure Security Agency ("CISA") 2020 guidance.

162. The FTC has brought enforcement actions against businesses for failing to reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[140]

163. Given the amount and sensitive nature of Private Information they store, Change Health Defendants recognize and have previously acknowledged their duty to comply with the legal requirements set forth in HIPAA and other regulations to protect health information received and/or collected via their clearinghouse networks.[141]

---

[139] *Start with Security, A Guide for Business*, FTC, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed Jan. 14, 2025).

[140] Privacy and Security Enforcement, FTC, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Jan. 14, 2025).

[141] *U.S. v. UnitedHealth Group Inc., and Change Healthcare Inc.*, 1:22-cv-481, Def.'s Proposed Findings of Fact and Conclusions of Law, ECF No. 121 at 44, 62 (D.D.C. Sept. 7, 2022).

c. Change Health Defendants represented that they adequately protected Private Information.

164. Change Health Defendants promise patients, Providers, and payers that they will keep sensitive patient data secure.

165. In its contracts with Providers, Change broadly represented that it would "retain in confidence and not disclose" "any and all confidential or proprietary information and materials" of the providers.[142] And with respect to PHI governed by HIPAA, Change specifically promised Providers that Change would "comply with federal and state laws regarding the protection of PHI as defined by HIPAA"[143] and "implement and maintain appropriate administrative, physical, and technical safeguards" to comply with the HIPAA Security Rule (45 C.F.R. Part 160 and Part 164, Subparts A and C) and to "prevent Use or Disclosure of [electronic PHI] other than as provided for by" Change's contracts with providers.[144] Change further told Providers that, if there were a data breach, it would report it to the Providers "without unreasonable delay" and in fewer than 14 days after discovery of a data breach.[145]

166. On its websites, Change also assures Providers that it has various processes and policies in place to protect their clients' and patients' sensitive information: "Keeping our customers' information secure is a top priority for Change Healthcare. We dedicate

[142] Change Healthcare Provider Complete Customer Agreement, ComplexCorp.Customer Agreement (version 01.2022), Section 6.2.
[143] *Id.*, Schedule B, Business Associate Agreement, Section 8.
[144] *Id.*, Schedule B, Business Associate Agreement, Section 3.1.
[145] *Id.*, Schedule B, Business Associate Agreement, Section 3.2.

extensive resources to make sure personal medical and financial information is secure and we strive to build a company culture that reinforces trust at every opportunity."[146]

167. Optum Insight's contracts with health insurers further require the company to protect customers' data, including PHI, and to "use all 'reasonable commercial means'" to do so.[147]

168. As part of the merger with Change, UHG made "binding commitments" to customers to apply and maintain data security policies to protect customers' data "and to uphold all contractual rights of Change's customers to audit the protection and security of their data."[148]

169. Given the extensive amount and sensitive nature of the data they handle, Change Health Defendants maintain privacy policies outlining the usage and disclosure of confidential and personal information.

170. Change's Global Privacy Notice represented that "Privacy matters to Change Healthcare, so we follow a privacy framework that helps us to manage and protect your personal information."[149] Change further represented that it implemented and maintained "security measures designed to safeguard the data we process against unauthorized access"

---

[146] Accreditations & Certifications, Change Healthcare, Sept. 20, 2021 (https://www.changehealthcare.com/accreditations-certifications) Internet Archive (https://web.archive.org/web/20240917185643/https://www.changehealthcare.com/accreditations-certifications).

[147] *U.S. v. UnitedHealth Group Inc., and Change Healthcare Inc.*, 1:22-cv-481, Def.'s Proposed Findings of Fact and Conclusions of Law, ECF No. 121 at 31 (D.D.C. Sept. 7, 2022).

[148] *Id.* at 107-108.

[149] Privacy Notice, Change Healthcare (Effective Date: Dec. 2023), https://www.changehealthcare.com/privacy-notice.html (last visited Jan. 15, 2025).

such that "Your Personal Information is only accessible to personnel who need to access it."[150]

171. Likewise, Change represents in its Code of Conduct[151] that:

a. "We exercise care and discretion when handling [restricted and confidential] information."

b. "We collect, store, access, use, share, transfer, and dispose of [personally identifiable information] responsibly."

c. "We also respect and protect the sensitive nature of [protected health information] and carefully maintain its confidentiality."

d. "We earn the trust of our team members and the companies with which we do business by following our privacy, security, and data and information protection policies."

e. "We also regularly monitor our systems to be sure that information is accessed and used for appropriate, authorized activities, to discover any new threats, and to look for ways to improve."

f. "We monitor and control all electronic and computing devices used … to interact with our internal networks and systems."

172. Hence, Change recognizes that its customers (i.e., Providers) and those they service have placed their trust in Change to protect the confidentiality and privacy of their

[150] *Id.* The Notice also defines "your" as used here to include the patients and consumers of the entity payer and provider customers for which it is a HIPAA business associate.

[151] Change Healthcare, Our Code of Conduct, Change Healthcare, at 15-17, https://codeofconduct.changehealthcare.com/ (last accessed Jan. 15, 2025).

data and "the consequences of betraying the trust of its customers…would be catastrophic."[152] Change is responsible to all those who place their trust in it to maintain data security, including the patients and consumers who are ultimately served by its Change Platform and Services.

173. UHG and Optum Insight adhere to the same "Privacy Policy," which assures the public—including patients and providers—that they have implemented "organizational, technical, and administrative security measures" to safeguard patients' information. Their "Social Security Number Protection Policy" explicitly states their commitment to preserving the confidentiality of Social Security numbers received or collected during business operations. UHG and Optum Insight also pledge to limit access to Social Security numbers to lawful purposes and to prohibit unlawful disclosure. Change similarly assures that it implements and maintains security measures—organizational, technical, and administrative—to protect processed data from unauthorized access, destruction, loss, alteration, or misuse. These measures aim to uphold the integrity and confidentiality of data, including personal information.[153]

174. Change Health Defendants represent to the public that these are not mere words or policies. Optum Insight's Chief Operating Officer has testified that the company's

[152] *U.S. v. UnitedHealth Group Inc., and Change Healthcare Inc.*, 1:22-cv-481, Def.'s Proposed Findings of Fact and Conclusions of Law, ECF No. 121 at 66 (D.D.C. Sept. 7, 2022) (internal quotations omitted).

[153] Privacy Notice, Change Healthcare, https://www.changehealthcare.com/privacy-notice (last visited Jan. 15, 2025).

culture is to "treat customers' data as they would treat their data themselves."[154] Change Health Defendants represented, under oath, that they had built a top down "culture of trust and integrity around protecting customers' sensitive information."[155]

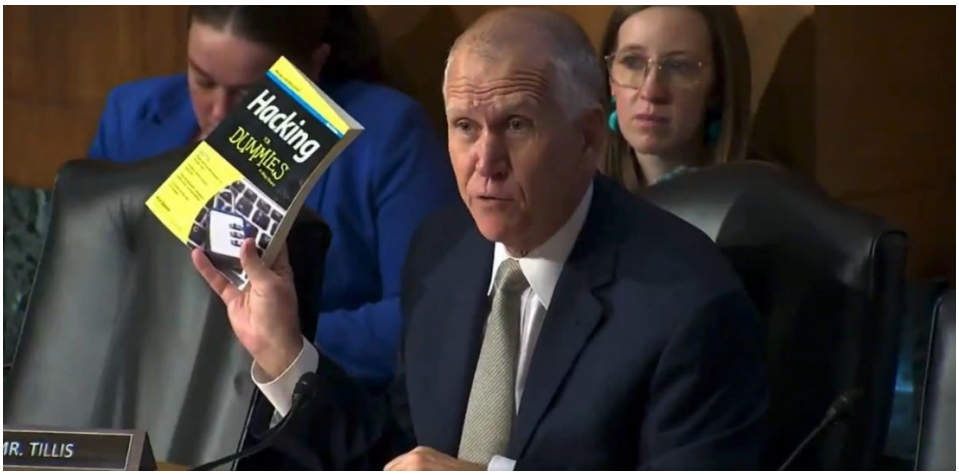
175. Given their representations and experience handling highly sensitive Private Information, Change Health Defendants understood the need and requirements to protect patients' Private Information and prioritize data security.

d. Change Health Defendants failed to comply with federal law and regulatory guidance to prevent the Data Breach and shutdown.

176. During a Senate hearing regarding the Ransomware Attack, Senator Wyden said, "the attack could have been stopped with 'Cybersecurity 101.'"[156] Senator Thom Tillis further confirmed the preventability of this Ransomware Attack. Waiving a paperback copy of "Hacking for Dummies," Senator Tillis emphasized that "[t]his is some basic stuff that was missed, so shame on internal audit, external audit and your systems folks tasked with redundancy, they're not doing their job."[157]

---

[154] *U.S. v. UnitedHealth Group Inc., and Change Healthcare Inc.*, No. 1:22-cv-481, Post-Trial Memorandum Opinion, ECF No. 138 at 40 (D.D.C. Sept. 21, 2022) (internal quotations omitted).
[155] *U.S. v. UnitedHealth Group Inc., and Change Healthcare Inc.*, No. 1:22-cv-481, Def.'s Proposed Findings of Fact and Conclusions of Law, ECF No. 121 at 30 (D.D.C. Sept. 7, 2022).
[156] Pietje Kobus, *UnitedHealth CEO Testifies on Cyberattack Before Senate*, Healthcare Innovation (May 2, 2024), https://www.hcinnovationgroup.com/cybersecurity/news/55036427/unitedhealth-ceo-testifies-on-cyberattack-before-senate (last accessed Jan. 14, 2025).
[157] UnitedHealth CEO Testifies Before Senate on Cyber Attack Against Change Healthcare, C-SPAN (April 30, 2024) at 01:13:42, available at https://www.c-span.org/program/public-affairs-event/unitedhealth-ceo-testifies-before-senate-on-cyber-attack-against-change-healthcare/641625?535259/unitedhealth-ceo-testifies-change-healthcare-cyber-attack-senate (last accessed Jan. 14, 2025).



177. Despite the foreseeability of the Ransomware Attack, this cyber disaster occurred because, as CEO Witty highlighted, Change employed outdated technology and UHG, UHCS, and Optum Insight failed to promptly fix Change's problems when UHG acquired Change Healthcare in October 2022.

178. Change Health Defendants' cybersecurity practices and policies were inadequate and fell short of the industry-standard measures that should have been implemented long before the Ransomware Attack occurred.

179. By marketing and advertising the Change Platform as a reliable, HIPAA-compliant solution for Providers and insurers handling highly sensitive Private Information, the Change Health Defendants assumed legal and equitable duties. The Change Health Defendants knew or should have known they were responsible for:

a. adequately designing, maintaining, and updating their software and networks;

b. promptly detecting, remediating, and notifying Providers and those they serve of any critical vulnerabilities in their software and networks;

c. ensuring compliance with industry standards related to data security;

d. ensuring compliance with regulatory requirements related to data security;

e. protecting and securing the Private Information stored on their networks from unauthorized disclosure; and

f. providing adequate notice to Providers and patients if patient Private Information is disclosed without authorization.

180. Change Health Defendants failed to use the requisite degree of care that a reasonably prudent company would use in designing, developing, and maintaining networks that perform a critical function in the healthcare system and store highly sensitive Private Information.

181. Despite their representations that the Change Platform complied with the requirements under HIPAA for data security, Change Health Defendants failed to:

a. Implement adequate procedures to verify that a person or entity seeking access to electronic PHI is the one claimed, in violation of 45 C.F.R. § 164(c).

b. Train all members of their workforces effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of Private Information, in violation of 45 C.F.R. § 164.530(b).

c. Implement a data security system that complied with the minimum necessary standard or principle of least privilege, thereby adequately limiting access to Private Information, in violation of 45 CFR §§ 164.502(b), 164.514(d).

d. Implement technical policies and procedures for electronic information systems that separate or segment data so that their systems allow access to Private Information only by those persons or software programs that have been granted access rights to, in violation of 45 C.F.R. § 164.312(a)(1).

e. Implement data security practices and procedures that adequately monitor network activity, such as reviewing records of information system activity regularly, including audit logs, access reports, and security incident tracking reports (45 C.F.R. § 164.308(a)(1)(ii)(D)), thereby preventing, detecting, containing, and correcting security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i).

f. Ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1).

g. Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3).

h. Ensure compliance with the electronically protected health information security standard rules by their workforces, in violation of 45 C.F.R. § 164.306(a)(4).

182. Change Health Defendants failed to implement each of the industry standard security protocols outlined below.

i. Change Health Defendants failed to implement multi-factor authentication for remote access to its servers.

183. Use of stolen credentials has long been the most popular and effective method of gaining authorized access to a company's internal networks. As a result, it is well-established that companies should take precautions to prevent attacks using stolen user credentials.

184. According to the FBI, phishing schemes designed to induce individuals to reveal personal information, such as network passwords, were the most common type of cybercrime in 2020, with such incidents nearly doubling in frequency between 2019 and 2020.[158] According to Verizon's 2021 Ransomware Attack Investigations Report, 43% of breaches stemmed from phishing and/or pretexting schemes.[159]

185. The risk is so prevalent for healthcare Providers that on October 28, 2020, the FBI and two federal agencies issued a "Joint Cybersecurity Advisory" warning that they have "credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers."[160]

---

[158] *2020 Internet Crime Report*, FBI Internet Complaint Center, available at https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (last accessed Jan. 14, 2025).

[159] *2021 DBIR Master's Guide*, Verizon, https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/ (subscription required) (last visited July 16, 2024).

[160] *Ransomware Activity Targeting the Healthcare and Public Health Sector*, Joint Security Advisory, Cybersecurity & Infrastructure Security Agency, FBI/U.S. Dept. of Justice, and U.S. Dept. of Health & Human Services (Updated Oct. 29, 2020), available at https://www.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf (last accessed Jan. 14, 2025).

186. Despite the apparent risk that a user's credentials could be compromised, Change Health Defendants failed to take reasonable steps to authenticate Change users.

187. In this context, "authentication" refers to steps a company can take which go beyond requiring the user to merely provide login name and password, namely steps which ensure that the person using the login and password is the person to whom the name and password were assigned. These steps can take the form of requiring the user to respond to a message on their phone, to physically toggle a device attached to their computer, to provide a fingerprint or other biometric information, to answer a phone call to their cell phone, or to take any other number of steps to confirm that the person using the login and password is authorized to do so.

188. Requiring more than just a login and password is referred to as Multifactor Authentication, or MFA. MFA is "an identity verification method in which a user must supply at least 2 pieces of evidence, such as their password and a temporary passcode, to prove their identity."[161] "For example, to log into an email account, a user might need to enter both their account password and a single-use passcode the email provider sends to their mobile phone via text message."[162] "MFA systems add an extra layer of security by requiring more than one piece of evidence to confirm a user's identity. Even if hackers steal a password, it won't be enough to gain unauthorized access to a system."[163]

[161] Matthew Kosinski & Amber Forrest, *What is MFA?*, IBM (Jan. 4, 2024), https://www.ibm.com/topics/multi-factor-authentication (last accessed Jan. 14, 2025).
[162] *Id.*
[163] *Id.*

189. At the time of the Ransomware Attack, Change employees could access Change's internal networks remotely through third-party Citrix Remote PC Access software.[164]

190. Citrix's "Remote PC Access is a feature of Citrix Virtual Apps and Desktops that enables organizations to easily allow their employees to access corporate resources remotely in a secure manner. The Citrix platform makes this secure access possible by giving users access to their physical office PCs. If users can access their office PCs, they can access all the applications, data, and resources they need to do their work."[165]

191. At the time of the Ransomware Attack, Change Health Defendants' implementation of Citrix Remote PC Access was not equipped with MFA.

192. MFA has existed since the 1980s[166] and has been widely in use since the late 2000s.[167] MFA using biometrics has been widely in use since the early 2010s.[168] MFA "has become an increasingly important piece of corporate identity and access management (IAM) strategies. Standard single-factor authentication methods, which rely on usernames

[164] Testimony of Andrew Witty Chief Executive Officer, UnitedHealth Group Before the House Energy and Commerce Committee Subcomittee on Oversight and Investigations, "*Examining the Change Healthcare Cyberattack*," UnitedHealth Group (May 1, 2024), available at https://www.congress.gov/118/meeting/house/117242/witnesses/HHRG-118-IF02-Wstate-WittyS-20240501-U5.pdf (last accessed Jan. 14, 2025).

[165] *Remote PC Access*, Citrix (Sept. 6, 2024), https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/install-configure/remote-pc-access.html (last visited Jan. 14, 2025).

[166] Caroline Delbert, *History of Online Security, from CAPTCHA to Multi-Factor Authentication*, Beyond Identity (May 31, 2022), https://www.beyondidentity.com/resource/history-of-online-security-from-captcha-to-multi-factor-authentication (last accessed Jan. 14, 2025).

[167] Rose de Fremery, *The Evolution of Multi-Factor Authentication*, LastPass (Dec. 22, 2021), https://blog.lastpass.com/posts/the-evolution-of-multi-factor-authentication (last accessed Jan. 14, 2025).

[168] *History of Authentication: From Zero to Hero*, ASEE (June 7, 2022), https://cybersecurity.asee.io/blog/history-of-authentication/ (last accessed Jan. 14, 2025).

and passwords, are easy to break. In fact, compromised credentials are one of the most common causes of data breaches, according to IBM's *Cost of a Ransomware Attack* report."[169]

193. In 2019, both Microsoft and Google publicly reported that using MFA blocks more than 99% of automated hacks, including most ransomware attacks that occur because of unauthorized account access. Likewise, the reputable SANS Software Security Institute issued a paper stating: "[t]ime to implement multi-factor authentication!"[170]

194. Citrix states on its website that "[i]t's critical . . . to also implement multi-factor authentication as a backup in case passwords do become compromised."[171]

195. HIPAA further requires covered entities to "[i]mplement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed." 45 C.F.R. § 164(c). MFA is widely recommended to meet this requirement for all healthcare applications.[172] The book *HIPAA Privacy and Security Compliance –*

---

[169] Matthew Kosinski & Amber Forrest, *What is MFA?*, IBM (Jan. 4, 2024), https://www.ibm.com/topics/multi-factor-authentication (last accessed Jan. 14, 2025).

[170] Matt Bromiley, *Bye Bye Passwords: New Ways to Authenticate*, SANS Software Security Inst. (July 2019), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3y9UJ (last accessed Jan. 14, 2025).

[171] *What is single sign-on (SSO)?*, Citrix, https://www.citrix.com/glossary/what-is-single-sign-on-sso.html (last visited Jan. 14, 2025).

[172] Marty Puranik, *Two-Factor Authentication: A Top Priority for HIPAA Compliance*, Techopedia (Aug. 25, 2023), https://www.techopedia.com/two-factor-authentication-a-top-priority-for-hipaa-compliance/2/33761 (last accessed Jan. 14, 2025); Utilizing Two Factor Authorization, HHS Cybersecurity Program, Office of Information Security, available at https://www.hhs.gov/sites/default/files/two-factor-authorization.pdf (last accessed Jan. 2, 2025); Liyanda Tembani, *Enhancing HIPAA compliance with multi-factor authentication*, Paubox (Aug. 9, 2024), https://www.paubox.com/blog/enhancing-hipaa-compliance-with-multi-factor-authentication (last accessed Jan. 14, 2025); Gil Vidals, *Multi-Factor Authentication For HIPAA Compliance: Securing Patient Data In The Digital Age*, HIPAAVault (Dec. 6, 2023),

Simplified: Practical Guide for Healthcare Providers and Managers states "Multi-factor authentications (MFA) shall be used for remote access, for system administration activities and for access to critical systems."[173]

196. MFA is also required by a number of other industry standards:

a. PCI-DSS The Payment Card Industry Data Security Standard requires multi-factor authentication per requirement 8.2.[174]

b. Service Organization Control 2 (SOC 2), a widely used cybersecurity auditing standard used for a wide range of businesses, requires multi-factor authentication.[175]

c. ISO 27002 is an international standard that provides guidance for organizations on how to establish, implement, and improve an Information Security Management System. ISO 27002 requires one to either use MFA, digital certificates, smart cards, or biometric login.[176]

---

https://www.hipaavault.com/hipaa-outlook/multi-factor-authentication-for-hipaa-compliance/ (last accessed Jan. 14, 2025).

[173] Robert Brzezinski, HIPAA Privacy and Security Compliance - Simplified: Practical Guide for Small and Medium Organizations 47 (2016 ed.).

[174] Information Supplement: Multi-Factor Authentication, PCI Security Standards Council (February 2017), available at https://listings.pcisecuritystandards.org/pdfs/Multi-Factor-Authentication-Guidance-v1.pdf (last accessed Jan. 14, 2025).

[175] Joe Ciancimino, *Comprehensive Guide to SOC 2 Controls List*, ISPartners (Nov. 2, 2023), https://www.ispartnersllc.com/blog/soc-2-controls/ (last accessed Jan. 14, 2025).

[176] ISO 27002:2022.Control 8.5 -Secure Authentication, ISMS Online, https://www.isms.online/iso-27002/control-8-5-secure-authentication/ (last visited Jan.14, 2025).

d. The Cybersecurity and Infrastructure Security Agency has strongly encouraged all businesses to use MFA for many years.[177]

e. NIST 800-53 strongly recommends multi-factor authentication beginning on page 132.[178] NIST 800-53 is a cybersecurity framework and compliance standard that can be used by any organization.

197. At the time of the Ransomware Attack, Change's internal networks were accessible through Citrix Remote PC Access without MFA, meaning that any third party that obtained a Change employee's login credentials could access Change's internal networks remotely.

198. Had Change Health Defendants had an MFA system in place, the Ransomware Attack and shutdown would have been prevented.

199. The failure to have MFA was an explicit violation of Change Health Defendants' own policies requiring MFA on all external-facing applications,[179] HIPAA, and the industry standards described above.

[177] Require Multifactor Authentication, Cybersecurity & Infrastructure Security Agency, U.S. Dept. of Homeland Security, https://www.cisa.gov/secure-our-world/require-multifactor-authentication (last visited Jan. 2, 2025).

[178] NIST Special Publication 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations, Natl. Institute of Standards and Tech., U.S. Dept. of Commerce, available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (last accessed Jan. 2, 2025).

[179] *Responses to Questions for the Record for Andrew Witty*, U.S. Senate Committee on Finance, Full Committee Hearing (May 1, 2024) at 1, available at https://www.finance.senate.gov/imo/media/doc/responses_for_questions_for_the_record_to_andrew_witty.pdf (last accessed Jan. 14, 2025).

ii. Change Health Defendants failed to apply the principle of least privilege to its systems.

200. The principle of least privilege is a cybersecurity concept that states a user or entity should only be granted the minimum access level needed to perform their required tasks, meaning they should only have access to the specific data, resources, and applications necessary to complete their job functions, and nothing more; essentially, providing the lowest level of privilege possible while still allowing them to do their work.

201. CISA and HIPAA require that the principle of least privilege be applied to all systems.[180]

202. HIPAA refers to this as the Minimum Necessary Rule.[181,] The Minimum Necessary Rule standard is based on the practice that PHI should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function. The Minimum Necessary Rule requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of PHI.

[180] Ransomware Guide September 2020, Cybersecurity & Infrastructure Security Agency, at 7-8, available at https://www.cisa.gov/sites/default/files/2023-01/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf (last accessed Jan. 14, 2025).

[181] 45 CFR 164.502(b), 164.514(d). *See also* Steve Alder, *The HIPAA Minimum Necessary Rule Standard*, The HIPAA Journal (Dec. 5, 2024), https://www.hipaajournal.com/ahima-hipaa-minimum-necessary-standard-3481/. *See also* Minimum Necessary, FAQs, U.S. Dept. of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/faq/minimum-necessary/index.html (last accessed Jan. 2, 2025).

203. Other applicable standards also require least privileges. For example, both *PCI-DSS requirement 7*,[182] and NIST 800-53 require least privileges.[183]

204. During the Ransomware Attack, the cybercriminals were able to use a low-level employee account to ultimately conduct administrator actions and move laterally throughout Change's networks and backup systems.

205. This low-level employee account should not have been configured in such a way as to allow it to create accounts with administrative privileges that could in turn be used to access and exfiltrate Private Information.

206. This low-level employee account should not have been configured in such a way as to allow it to create accounts with administrative privileges that could in turn be used to encrypt the Change Platform.

207. Change Health Defendants did not adequately follow the principle of least privilege or the Minimum Necessary Rule.

---

[182] PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.1, PCI Security Standards Council (May 2015), available at https://listings.pcisecuritystandards.org/documents/PCIDSS_QRGv3_1.pdf (last accessed Jan. 14, 2025); Surkay Baykara, *PCI DSS Requirement 7 Explained*, PCI DSS Guide (April 7, 2020), https://pcidssguide.com/pci-dss-requirement-7/ (last accessed Jan. 2, 2025); *How to Comply with PCI DSS Compliance Requirement 7*, Indent (Dec. 6, 2023), https://indent.com/blog/pci-dss-requirement-7 (last accessed Jan. 14, 2025).

[183] Tony Goulding, *What you need to know about NIST 800-53, least privilege, and PAM*, Delinea, https://delinea.com/blog/nist-800-53-security-privacy-privileged-access (last accessed Jan. 2, 2025); NIST Special Publication 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations, Natl. Institute of Standards and Tech., U.S. Dept. of Commerce, available at https://csrc.nist.gov/CSRC/media/Projects/risk-management/800-53%20Downloads/800-53r5/SP_800-53_v5_1-derived-OSCAL.pdf (last accessed Jan. 2, 2025); Asif Ali, *What you need to know about NIST 800-53, least privilege, and PAM*, AuthNull (last updated Sept. 8, 2024), https://authnull.com/blog/posts/What-you-need-to-know-about-NIST-800-53,-least-privilege,-and-PAM/ (last accessed Jan. 14, 2025)

208. Had Change Health Defendants adequately implemented policies and procedures applying the principle of least privilege or the Minimum Necessary Rule, the Ransomware Attack and shutdown could have been prevented.

iii. Change Health Defendants did not properly segment Change's systems.

209. Change Health Defendants should have also properly siloed the systems so that a bad actor would be unable to escalate privileges and move laterally through Change's systems.

210. This data security procedure is called segmentation. Data silos are created when an organization manages different types of data and software separately, without maintaining a centralized system to share and access information.[184] Each data silo or segment should have its own security defense mechanisms so that breaching one segment does not give an attacker access to other segments.

211. CISA guidance recommends that using a comprehensive network, in addition to network segregation, will help contain the impact of an intrusion and prevent or limit lateral movement on the part of malicious actors.[185]

[184] Ransomware Guide September 2020, Cybersecurity & Infrastructure Security Agency, at 7-8, available at https://www.cisa.gov/sites/default/files/2023-01/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf (last accessed Jan. 14, 2025); *see also* Robert Wood, *Why Data Silos Create Cybersecurity Risks and How to Break Them Down*, Acceleration Economy (Feb. 27, 2023), https://accelerationeconomy.com/cybersecurity/why-data-silos-create-cybersecurity-risks-and-how-to-break-them-down/# (last accessed Jan. 14, 2025).

[185] Ransomware Guide September 2020, Cybersecurity & Infrastructure Security Agency, available at https://www.cisa.gov/sites/default/files/2023-01/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf (last accessed Jan. 14, 2025).

212. During the Ransomware Attack, the cybercriminals were able to access patients' Private Information, Change software, Change's backup systems, and more. The breadth of access the attackers had demonstrates that Change Health Defendants did not properly implement network segmentation.

213. The lack of segmented systems allowed the hacker to travel among Change's systems freely, compromising multiple systems which Change Health Defendants were unable to recover, and ultimately resulting in the complete shutdown of Change's operations.

214. Had Change Health Defendants adequately implemented data segmentation, the Ransomware Attack and shutdown would have been prevented, or would have been much smaller in scope.

iv. Change Health Defendants failed to protect their backup technology and data.

215. IT Redundancy helps companies mitigate the effects of a ransomware attack. IT Redundancy means "[p]rovision of duplicate, backup equipment or links that immediately take over the function of equipment or transmission lines that fail."[186] So for example, if a primary server fails, a backup server can take over, ensuring that patient data is still accessible and that critical healthcare services can continue.

[186] *Redundancy*, Information Technology Glossary, Gartner https://www.gartner.com/en/information-technology/glossary/redundancy (last accessed Jan. 14, 2025).

216. Organizations like the AHA recommend companies in the healthcare industry use "backup technology which renders the backups 'immutable' – unable to be deleted, altered or encrypted."[187]

217. Unfortunately, like their data security, Change Health Defendants' IT Redundancy was also subpar. As Senator Wyden emphasized, "[m]ultifactor authentication is vital for prevention, but redundancies . . . help the company get back on its feet . . . [Change Health Defendants] flunked both."[188]

218. Once Change's system was infiltrated, ALPHV was allowed to disable both the primary and backup systems for the Change Platform because the backup systems were not immutable nor isolated from the primary systems, and few elements were stored on the cloud. These are all elementary security features that Change Health Defendants should have employed to prevent the disastrous effects of the Ransomware Attack.

219. Had Change Health Defendants adequately protected Change's backup technology and data, the shutdown would have been prevented.

---

[187] AHA Cybersecurity Advisory, *UnitedHealth Group's Change Healthcare Experiencing Cyberattack that Could Impact Health Care Providers*, American Hospital Association (Feb. 22, 2024), https://www.aha.org/advisory/2024-02-22-unitedhealth-groups-change-healthcare-experiencing-cyberattack-could-impact-health-care-providers-and (last accessed Jan. 14, 2025).

[188] Jessie Hellmann, *UnitedHealth Group CEO blames hack on aged technology systems*, Roll Call (May 1, 2024, 5:52 PM), https://rollcall.com/2024/05/01/unitedhealth-group-ceo-blames-hack-on-aged-technology-systems/ (last accessed Jan. 14, 2025).

v. Change Health Defendants failed to implement critical internal cybersecurity monitoring at Change.

220. At the time of the Ransomware Attack, Change Health Defendants did not have adequate cybersecurity monitoring systems in place to prevent and detect unauthorized access to the Change networks.

221. Change, like any entity in the healthcare industry storing valuable data, should have had robust protections in place to detect and terminate a successful intrusion long before access and exfiltration could expand to millions of patient files. Change Health Defendants' below-industry-standard procedures and policies are inexcusable given their knowledge that they were a prime target for cyberattacks.

222. "Cybersecurity or process monitoring is continuously observing and analyzing your computer network or systems to prevent cyberattacks. The primary objective of monitoring in cybersecurity is quickly identifying signs of vulnerability and responding to potential security threats in real-time."[189]

223. A key component of cybersecurity monitoring is an intrusion detection system (IDS), which "analyzes an organization's network traffic, activities, and devices, looking for known malicious activities or policy violations. If an IDS detects suspicious activities or patterns, it alerts the system administrators or security team of the potential threat."[190]

---

[189] *Cyber Security Monitoring: Definition and Best Practices*, SentinelOne (Oct. 16, 2024), https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-monitoring/ (last visited Jan. 14, 2025).

[190] *Id*.

224. Another "[o]ne of the simplest yet effective methods of safeguarding systems is through IP whitelisting. It is particularly beneficial for businesses that rely on remote access or have distributed teams but want to maintain strict security protocols. . . . IP whitelisting is a security practice that involves creating a list of trusted IP addresses granted access to a specific server, application, or network. By using IP whitelisting, only pre-approved IP addresses can interact with your system. By restricting access to a select group of devices based on their IP addresses, you can limit exposure to potential attacks and unauthorized access. The method effectively controls access to critical business systems, cloud infrastructure, and online services."[191]

225. NIST Special Publication 800-167: *Guide to Application Whitelisting* provides specific guidance to companies on how to implement whitelisting.[192]

226. The CISA guidance also encourages organizations to prevent unauthorized access by:

a. Conducting regular vulnerability scanning to identify and address vulnerabilities, particularly on internet-facing devices;

b. Regularly patching and updating software to latest available versions, prioritizing timely patching of internet-facing servers and software processing internet data;

[191] Timothy Shim, *IP Whitelisting: The Beginner's Guide*, Rapid Seedbox, (Oct. 7, 2024), https://www.rapidseedbox.com/blog/ip-whitelisting/ (last accessed Jan. 14, 2025).
[192] U.S. Dept. of Commerce, NIST Special Publication 800-167, *Guide to Application Whitelisting*, (Oct. 2015), available at https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-167.pdf (last accessed Jan. 14, 2025).

c. Ensuring devices are properly configured and that security features are enabled;

d. Employing best practices for use of Remote Desktop Protocol (RDP) as threat actors often gain initial access to a network through exposed and poorly secured remote services; and

e. Disabling operating system network file sharing protocol known as Server Message Block (SMB), which is used by threat actors to travel through a network to spread malware or access sensitive data.[193]

227. The CISA guidance further recommends implementing a real-time intrusion detection system that will detect potentially malicious network activity that occurs prior to ransomware deployment.[194]

228. Change's systems lacked internal monitoring to such a degree that the attackers were not detected until they chose to reveal themselves—nine days after gaining access.

229. ALPHV's activity involved several steps that should have been noticed by Change Health Defendants through proper endpoint and network monitoring and scanning. This includes:

[193] Ransomware Guide September 2020, Cybersecurity & Infrastructure Security Agency, at 4, available at https://www.cisa.gov/sites/default/files/2023-01/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf (last accessed Jan. 14, 2025).
[194] *Id.* at 5.

a. Installing software such as nmap, an obvious and 'noisy' network discovery scanner.[195] Only administrators should be able to install any software, and then such installations should still be monitored.[196] Had Change Health Defendants properly monitored Change's systems, they would not have allowed nmap to be installed in the first instance. A properly monitored network would have also detected nmap being installed. Application whitelisting, which means even administrators can only install software that has been pre-approved[197] would have also prevented the installation of nmap because nmap would not have been on the whitelist.

b. The attackers also ran several administrator-only commands. These commands should only be possible for those with the highest security privileges, and even then, the execution of these privileges should be logged and monitored. Had Change Health Defendants had proper monitoring on the

[195] Daryna Olyniychuk, *Detect ALPHA SPIDER Ransomware Attacks: TTPs Leveraged by ALPHV aka BlackCat RaaS Operators*, SOC Prime (March 15, 2024), https://socprime.com/blog/detect-alpha-spider-ransomware-attacks-analysing-ttps-leveraged-by-alphv-BlackCat-raas-operators/ (last accessed Jan. 14, 2025).

[196] Limit Software Installation, Mitre Att&ck (last updated Oct. 17, 2024), https://attack.mitre.org/mitigations/M1033/ (last visited Jan. 14, 2025); Restrict Software on Windows Devices Using a Policy, Jumpcloud, https://jumpcloud.com/support/restrict-software-on-windows-devices-using-policy (last accessed Jan. 2, 2025); *What Is a Software Restriction Policy?*, Heimdal (last updated Dec. 8, 2023), https://heimdalsecurity.com/blog/software-restriction-policy/ (last visited Jan. 14, 2025).

[197] *Protecting Against Malicious Code*, Cybersecurity & Infrastructure Security Agency, U.S. Dept. of Homeland Security (last updated Nov. 19, 2019), https://www.cisa.gov/news-events/news/protecting-against-malicious-code (last accessed Jan. 14, 2025); Katie C. Stewart, *Establish and Maintain Whitelists*, Software Engineering Institute, Carnegie Mellon University (Oct. 25, 2017), available at https://insights.sei.cmu.edu/blog/establish-and-maintain-whitelists-part-5-of-7-mitigating-risks-of-unsupported-operating-systems/ (last accessed Jan. 14, 2025).

networks, the administrator-only commands would have alerted Change Health Defendants' IT personnel.

c. The attackers exfiltrated terabytes of Private Information. Such actions should have only been possible by Change Health Defendants' network administrators and should have required even administrators to pass additional security features. Such exfiltration activity should have been detected and raised numerous red flags within the system.

230. Had Change Health Defendants implemented adequate internal cybersecurity monitoring, the Ransomware Attack and shutdown would have been prevented or much smaller in scope.

vi. Change Health Defendants failed to protect against known threats from the ALPHV cybercriminal ransomware group.

231. Not only would proper endpoint and network monitoring have detected and alerted Change Health Defendants to software installation, privilege escalation, and exfiltration, Change Health Defendants also should have properly configured Change's networks to detect and block this specific ALPHV/Blackcat ransomware attack. The attackers were well-known to target participants in the healthcare industry, and employed certain signature technologies and methods that Change Health Defendants could have configured Change's systems to detect and stop.

232. "ALPHV operates as a Ransomware-as-a-Service (RaaS), which means fellow threat actors can become affiliates by purchasing access to ALPHV ransomware,

infrastructure, and other resources. ALPHV affiliates conduct attacks, while ALPHV focuses on affiliate support, ransomware development, and business expansion."[198]

233. ALPHV is notably sophisticated in its use of the Rust programming language, "which improve[s] attack performance."[199]

234. ALPHV cybersecurity attacks often use the "double extortion" method, whereby a victim's data is both ransomed—*i.e.*, stolen with the threat of publication if a ransom is not paid—and encrypted—*i.e.*, turned into an unreadable format on the victim's network, so that the victim cannot continue using the data without ALPHV's decryption key.[200]

235. ALPHV also sometimes use "triple extortion" which additionally adds the threat of distributed denial of service (DDoS) attack, which can shut down a victim's networks.[201]

236. By 2023, ALPHV had collected nearly $300 million in ransom and gained notoriety for high-profile attacks targeting healthcare entities specifically.[202]

237. At the time of the Ransomware Attack, the U.S. Department of State was "offering a reward of up to $10,000,000 for information leading to the identification or

[198] Christine Barry, *ALPHV-BlackCat ransomware group goes dark*, Barracuda (Mar. 7, 2024), available at https://blog.barracuda.com/2024/03/06/alphv-blackcat-ransomware-goes-dark (last accessed Jan. 14, 2025).
[199] *Id.*
[200] *Id.*
[201] *Id.*
[202] *Id.*

location of any individual(s) who hold a key leadership position in the Transnational Organized Crime group behind the ALPHV/BlackCat ransomware variant."[203]

238. The U.S. Department of Health and Human Services has recognized ALPHV ransomware as a sophisticated threat to the health sector since at least 2023.[204]

239. In January 2023, Nextgen Health, a "multibillion-dollar healthcare giant [that] produces electronic health record (EHR) software and practice management systems for hundreds of the biggest hospitals and clinics in the U.S.," was attacked by ALPHV ransomware.[205]

240. In February 2023, ALPHV successfully penetrated the Lehigh Valley Health Network systems and exfiltrated and published sensitive patient data including clinical images of breast cancer patients that the group notoriously teased as "nude photos."[206]

241. In July 2023, ALPHV attacked Barts Health NHS Trust in the UK and exfiltrated seven terabytes of information.[207]

---

[203] Reward for Information: ALPHV/Blackcat Ransomware as a Service, U.S. Dept. of State (Feb. 15, 2024), https://www.state.gov/reward-for-information-alphv-blackcat-ransomware-as-a-service/ (last visited Jan. 14, 2025).

[204] *Royal & BlackCat Ransomware: The Threat to the Health Sector*, U.S. Dep't of Health and Human Servs. (Jan. 12, 2023), available at https://www.hhs.gov/sites/default/files/royal-blackcat-ransomware-tlpclear.pdf (last accessed Jan. 14, 2025).

[205] Jonathan Greig, *Electronic health record giant NextGen dealing with cyberattack*, The Record (Jan. 19, 2023), available at https://therecord.media/electronic-health-record-giant-nextgen-dealing-with-cyberattack (last accessed Jan. 14, 2025).

[206] Alexander Martin, *Ransomware gang posts breast cancer patients' clinical photographs*, The Record (Mar. 6, 2023), available at https://therecord.media/ransomware-lehigh-valley-alphv-black-cat (last accessed Jan. 14, 2025).

[207] *BlackCat/ALPHV Ransomware: In-Depth Analysis and Mitigation*, Stonefly, https://stonefly.com/blog/BlackCat-alphv-ransomware-analysis-and-mitigation/ (last accessed Jan. 2, 2025).

242. In October 2023, ALPHV took credit for a July 2023 attack on McLaren Health Care, where they successfully exfiltrated the Private Information of over 2.2 million McLaren patients.[208]

243. According to John Riggi, the AHA's national advisor for cybersecurity and risk, as of December 20, 2023 "[ALPHV] has attacked numerous hospitals, publicly exposed sensitive patient data and placed patient care and lives at risk."[209]

244. On December 19, 2023 the FBI and CISA co-authored a Joint Cybersecurity Advisory titled "#StopRansomware: ALPHV BlackCat" warning that ALPHV was targeting critical infrastructure with ransomware.

245. The Advisory identified certain Indicators of Compromise ("IoCs") associated with the ransomware group.[210]

246. Typical IoCs are virus signatures and IP addresses, MD5 hashes of malware files, or URLs or domain names of botnet command and control servers. After IoCs have been identified they can be used for early detection of future attack attempts using intrusion detection systems and antivirus software.

---

[208] Bill Toulas, *McLaren Health Care says ransomware attack impacted 2.2 million people* (Nov. 10, 2023), available at https://www.bleepingcomputer.com/news/security/mclaren-health-care-says-data-breach-impacted-22-million-people/ (last accessed Jan. 14, 2025).

[209] *DOJ disrupts ALPHV/BlackCat ransomware group*, AHA News (Dec. 20, 2023), available at https://www.aha.org/news/headline/2023-12-20-doj-disrupts-alphvBlackCat-ransomware-group (last accessed Jan. 14, 2025).

[210] *Joint Cybersecurity Advisory TLP Clear: #StopRansomware: ALPHV BlackCat* (Dec. 19, 2023), available at: https://www.aha.org/cybersecurity-government-intelligence-reports/2023-12-19-joint-cybersecurity-advisory-tlp-clear-stopransomware-alphv-blackcat (last accessed Jan. 14, 2025).

247. The FBI and CISA Advisory specifically noted that "[s]ince previous reporting, ALPHV BlackCat actors released a new version of the malware, and the FBI identified over 1000 victims worldwide [nearly 75 percent of which are in the United States] targeted via ransomware and/or data extortion."

248. The Advisory further recommended that potential targets implement specific precautions to "to improve your organization's cybersecurity posture based on threat actor activity and to reduce the risk of compromise by ALPHV BlackCat threat actors."

249. As far back as 2022 and continuing to 2023, independent security researchers also published guides detailing ALPHV's IoCs, and specific prophylactic measures organizations could implement to detect, prevent, or mitigate the group's ransomware attacks.[211] Moreover, ALPHV was infecting systems that did not use multi-factor authentication at least as early as 2022.[212]

250. As described, the steps of an ALPHV attack are well-documented, as are the defenses that can be employed at each step to foil an attack. An overview of a standard process is given here: [213]

---

[211] *BlackCat/ALPHV Ransomware: In-Depth Analysis and Mitigation*, Stonefly, https://stonefly.com/blog/BlackCat-alphv-ransomware-analysis-and-mitigation/ (last accessed Jan. 2, 2025); Amanda Tanner, *Threat Assessment: BlackCat Ransomware* (Jan. 27, 2022) https://unit42.paloaltonetworks.com/BlackCat-ransomware/ (last visited Jan. 14, 2025).

[212] Daryna Olyniychuk, *Detect ALPHA SPIDER Ransomware Attacks: TTPs Leveraged by ALPHV aka BlackCat RaaS Operators*, SOC Prime (March 15, 2024), https://socprime.com/blog/detect-alpha-spider-ransomware-attacks-analysing-ttps-leveraged-by-alphv-BlackCat-raas-operators/ (last accessed Jan. 14, 2025).

[213] *A Deep Dive Into ALPHV/BlackCat Ransomware*, SecurityScorecard, https://securityscorecard.com/research/deep-dive-into-alphv-BlackCat-ransomware (last accessed Jan. 2, 2025); *What is BlackCat Ransomware*, Akamai, https://www.akamai.com/glossary/what-is-BlackCat-ransomware (last accessed Jan. 2, 2025); Mehardeep Singh Sawhney, *Technical*

a. Initial access often begins with obtaining login credentials and exploiting systems that do not have MFA.

b. After access is achieved, the network is scanned for other machines. A network scan, particularly using such a widely known tool as nmap, should be detected by any properly configured system monitoring.

c. They next use a tool named PsExec[214] to deploy additional malware to other systems on the network. This tool is a free tool but must be downloaded and installed on the machine. If the victim systems are using the very fundamental cybersecurity principle of least privilege, then only a select few accounts would even be able to install software. This would mean that if the attackers gained access through an account that was not part of the group that had privileges to install software, their attack would be stopped.

d. The tool the attackers deploy is ExMatter.[215] It is a tool written in .Net specifically to exfiltrate data. Specifically, ExMatter will steal user files, compressed files, and databases, then upload them to a Secure File Transfer

Analysis of ALPHV/BlackCat Ransomware, CloudSek (May 22, 2023), https://www.cloudsek.com/blog/technical-analysis-of-alphv-BlackCat-ransomware (last accessed Jan. 14, 2025); *BlackCat/ALPHV Ransomware: In-Depth Analysis and Mitigation*, Stonefly, https://stonefly.com/blog/BlackCat-alphv-ransomware-analysis-and-mitigation/ (last accessed Jan. 2, 2025); Jason Hill, *BlackCat Ransomware (ALPHV)*, Varonis (last updated April 14, 2023) https://www.varonis.com/blog/BlackCat-ransomware (last accessed Jan. 14, 2025).

[214] Mark Russinovich, *PsExec v2.43*, Microsoft Learn, Systerinals (April 11, 2023), available at https://learn.microsoft.com/en-us/sysinternals/downloads/psexec (last accessed Jan. 14, 2025).

[215] ExMatter, Malpedia, https://malpedia.caad.fkie.fraunhofer.de/details/win.exmatter (last accessed Jan. 2, 2025).

Protocol server (SFTP).[216] Properly managed systems should notice any system initiating an SFTP transfer to outside the network.

e. ALPHV will also run a number of commands, all of which should require administrative privileges in a properly configured network:

1. Get device UUID
2. Stop IIS service
3. Clean Shadow Copies
4. List Windows Event logs and try to clear them (this in particular should trigger some monitoring system).

f. Only then does ALPHV encrypt the files.

251. HIPAA security standards require organizations to "[p]rotect against any reasonably anticipated threats or hazards to the security or integrity of such information."[217] Automatically tracking IoCs is a standard method for companies to comply with these requirements.[218]

[216] *Analyzing Exmatter: A Ransomware Data Exfiltration Tool*, Kroll (Mar. 22, 2022), available at https://www.kroll.com/en/insights/publications/cyber/analyzing-exmatter-ransomware-data-exfiltration-tool (last accessed Jan. 14, 2025).
[217] 45 C.F.R. § 164.306(a)(2).
[218] Robert Brzezinski, HIPAA Privacy and Security Compliance - Simplified: Practical Guide for Small and Medium Organizations 28 (2016 ed.); SecurityMetrics Guide to HIPAA Compliance (8th ed.), available at: https://www.securitymetrics.com/content/dam/securitymetrics/PDF-files/SecurityMetrics_Guide_to_HIPAA_Compliance_Eighth_Edition.pdf (last accessed Jan. 2, 2025); Technical Vol. 2: Cybersecurity Practices for Medium and Large Healthcare Organizations 2023 Edition, Healthcare & Public Health Sector Coordinating Council, U.S. Dept. of Health & Human Services, available at: https://405d.hhs.gov/Documents/tech-vol2-508.pdf (last accessed Jan. 2, 2025).

252. At the time of the Ransomware Attack, ALPHV was a reasonably anticipated threat or hazard to the Change Health Defendants.

253. Change Health Defendants knew or should have known of their obligation to implement and use reasonable measures to protect against ALPHV attacks.

254. As evidenced by the Ransomware Attack, Change Health Defendants did not track IoCs regarding ALPHV or implement other reasonable measures to prevent an ALPHV attack.

255. Had Change Health Defendants tracked ALPHV IoCs and implemented measures to detect and ALPHV attack, the Ransomware Attack could have been prevented.

vii. Change Health Defendants did not properly encrypt or hash Private Information.

256. HIPAA recommends appropriately encrypting data using a robust encryption algorithm, whether at rest or in transition.

257. For organizations like Change, with abundant technology resources, HIPAA regulations require encryption of PHI and dictate that all encryption protocols follow the NIST standards.

258. For example, NIST 800-53 recommends removing, masking, encrypting, or hashing PII contained in company datasets.[219] "There are many possible processes for removing direct identifiers from a dataset. Columns in a dataset that contain a direct

[219] NIST Special Publication 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations, Natl. Institute of Standards and Tech., U.S. Dept. of Commerce, available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (last accessed Jan. 2, 2025).

identifier can be removed. In masking, the direct identifier is transformed into a repeating character, such as XXXXXX or 999999. Identifiers can be encrypted or hashed so that the linked records remain linked. In the case of encryption or hashing, algorithms are employed that require the use of a key, including the Advanced Encryption Standard or a Hash-based Message Authentication Code. Implementations may use the same key for all identifiers or use a different key for each identifier. Using a different key for each identifier provides a higher degree of security and privacy. Identifiers can alternatively be replaced with a keyword, including transforming 'George Washington' to 'PATIENT' or replacing it with a surrogate value, such as transforming 'George Washington' to 'Abraham Polk.'"

259. Change Health Defendants were fully aware of their obligations to implement and use reasonable measures such as encryption to protect patients' Private Information.

260. Given the attackers were able to access Private Information, Change Health Defendants failed to comply with these basic recommendations and guidelines and did not protect Private Information with sufficient masking, encrypting, or hashing.

261. Change Health Defendants' failure to employ reasonable measures to protect against unauthorized access to patient information violated HIPAA and constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

262. Had Change Health Defendants adequately encrypted or hashed Private Information, the Ransomware Attack and shutdown would have been prevented.

NAMED PLAINTIFF

263. The Plaintiff identified below brings this action on behalf of itself and those similarly situated in the classes identified below. Plaintiff is a Provider whose business operations was disrupted when Change Health Defendants disconnected the Change Platform as a belated attempt to stop the Ransomware Attack caused by their own failures.

264. At the time of the shutdown, Plaintiff used and relied on the Change Platform to facilitate processing of insurance claims for approval and payment.

265. It was foreseeable that Change Health Defendants' substandard network security and failure to establish a reliable backup system would result in the Change Platform becoming non-operational in the event of a cyberattack or ransomware attack. Had Change Health Defendants disclosed their network security was not compliant with HIPAA and other industry standards. and that they did not have a reliable backup system, Plaintiff would not have used the Change Platform.

266. Plaintiff Odom Health & Wellness is a sports medicine, physical therapy, and wellness practice located and registered in Eden Prairie, Minnesota.

267. Plaintiff, through a third-party intermediary, relied on Change to provide the Services, such as processing medical claims, to Plaintiff so that Plaintiff could receive payment for medical care provided to its patients.

268. Because of Change Health Defendants' substandard data security measures, Change experienced the Ransomware Attack. In response, Change Health Defendants chose to disconnect the Change Platform. As a result of Change Health Defendants' decision to disconnect the Change Platform, Plaintiff was unable to submit claims, receive

ERAs, and receive payment for its medical care to patients. Plaintiff's business was thereby disrupted and still has not recovered to pre-Ransomware Attack conditions.

269. As a result of Change Health Defendants' actions, Plaintiff did not receive the services it paid for from Change. In addition, this business disruption has caused Plaintiff to suffer monetary losses, such as rejected and/or delayed payments for medical care thus depriving Plaintiff of the time value of money and loss of interest. Furthermore, Plaintiff spent significant time and resources, including but not limited to investigating the network outage and alternative methods to receive payment for medical care, which increased manual labor costs.

270. Because of these monetary losses and business disruption, Plaintiff was forced to participate in the TFAP, where Plaintiff received an advance of $569,680.00 to be paid back when Plaintiff's collections pursuant to its submitted medical claims were current.

271. If Plaintiff knew about Change Health Defendants' inadequate data security practices, it would have attempted to use an alternative to the Change Platform.

CLASS ACTION ALLEGATIONS

272. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiff seeks certification of the following nationwide classes (the "Nationwide Classes" or the "Classes"):

> National Providers Class: All Providers whose use of Change's Services, either directly or indirectly, was disrupted, or whose payments were delayed or denied because of the Ransomware Attack and shutdown.

> National Provider Loan Assistance Sub-Class: Members of the National Providers Class that accepted a Temporary Funding Assistance Program loan from Defendants.

273. Pursuant to Fed. R. Civ. P. 23, Plaintiff also seeks certification of state claims in the alternative to the nationwide claims, as well as statutory claims under state data breach statute and consumer protection statute, on behalf of a separate statewide Class for Minnesota (the "Statewide Class" or "Minnesota State Class"), defined as follows:

> Minnesota Class: All Providers residing in Minnesota whose use of Change's Services was disrupted, or whose payments were delayed because of the Ransomware Attack and shutdown.

The foregoing Statewide Class, together with the Nationwide Classes, are referred to collectively as the "Class" herein.

274. Excluded from the proposed Class are Defendants, any entity in which Defendants have a controlling interest, is a parent or subsidiary, or which is controlled by Defendants, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendants. Also excluded from the Class are any federal, state, or local governmental entities, any judicial officer presiding over this action and the members of their immediate family and judicial staff, and any juror assigned to this action.

275. **Class Identity**: The Class members are readily identifiable and ascertainable. Defendants and/or their affiliates, among others, possess the information to identify and contact Class members.

276. **Numerosity**: The Class members are so numerous that joinder of all of them is impracticable. According to the U.S. Department of Health and Human Services, Change "processes 15 billion health care transactions annually and is involved in one in every three patient records." According to Change, it is connected to "more than 800,000 providers[.]"

277. **Typicality**: Plaintiff's claims are typical of the claims of the Class members because all Class members could not submit medical claims through Change Health Defendants' Change Platform or were delayed or denied payment because of the Ransomware Attack and shutdown and were harmed as a result.

278. **Adequacy**: Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff has no known interests antagonistic to those of the Class members and its interests are aligned with Class members' interests. Plaintiff could not submit medical claims through Change Health Defendants' Change Platform and/or its payments were delayed or denied because of the Ransomware Attack and shutdown just as Class members were, and suffered similar harms. Plaintiff has also retained competent counsel with significant experience litigating complex and commercial class actions.

279. **Commonality and Predominance**: There are questions of law and fact common to the Class members such that there is a well-defined community of interest in this litigation. These common questions predominate over any questions affecting only individual Class members. The common questions of law and fact include, without limitation:

(a) Whether Change Health Defendants owed Plaintiff and Class members a duty to implement and maintain reasonable security procedures and practices to protect patients' Private Information;

(b) Whether Change Health Defendants received a benefit without proper restitution making it unjust for Change Health Defendants to retain the benefit without commensurate compensation;

(c) Whether Change Health Defendants acted negligently by not implementing adequate security systems to ensure their network was not disconnected;

(d) Whether Change Health Defendants violated their duty to implement adequate security systems to ensure their network was not disconnected;

(e) Whether Change Health Defendants' breaches of their duties to implement reasonable security systems directly and/or proximately caused damages to Plaintiff and Class members;

(f) Whether Change Health Defendants adequately addressed and fixed the vulnerabilities that enabled the Ransomware Attack;

(g) Whether Defendants breached agreements with Plaintiff and Class members by disconnecting the Change Platform and demanding payment on TFAP loans; and

(h) Whether Class members are entitled to compensatory damages, punitive damages, and/or statutory or civil penalties as a result of the Ransomware Attack and shutdown.

280. Defendants have engaged in a common course of conduct and Plaintiff and Class members have been similarly impacted by Change Health Defendants' failure to maintain reasonable security procedures and practices.

281. **Superiority**: A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most if not all Class members would find the cost of litigating their individual claims prohibitively high and have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members and risk inconsistent treatment of claims arising from the same set of facts and occurrences. Plaintiff knows of no difficulty likely to be encountered in the maintenance of this action as a class action under the applicable rules.

CLAIMS FOR RELIEF
COUNT I: NEGLIGENCE
(On Behalf of Plaintiff and the National Providers Class, or Alternatively, the Statewide Class, Against the Change Health Defendants)

282. Plaintiff repeats and realleges every allegation set forth in Paragraphs 1 to 281.

283. At relevant times, Change Health Defendants set up, provided, managed, maintained, operated, supervised, controlled, and commercially benefited from a network, equipment, and systems ("System") used to operate the Change Platform and offer the Services to Plaintiff and Class members.

284. Each of the Change Health Defendants owed Plaintiff and Class members a duty to exercise reasonable care in setting up, providing, managing, maintaining, operating, supervising, and controlling the System, including a duty to secure the System against reasonably foreseeable breaches of the System, to have adequate training and policies to secure the System against reasonably foreseeable ransomware attacks, to warn Plaintiff (directly or through their vendors) of gaps or deficiencies in the System, to monitor the System for attacks, to timely notify Plaintiff (directly or through their vendors) of attacks, and to ensure that the Services would be properly functioning, timely, and accurate, including by having redundancies and contingency plans in the event of an attack on the System.

285. Change Health Defendants also owed Plaintiff and Class members a duty to exercise reasonable care to avoid harm to Plaintiff and Class members because they were reasonably foreseeable and probable victims of substandard cybersecurity practices, such as a lack of MFA, given that Change Health Defendants' System houses the Services such that it was reasonably foreseeable that, if an attack on the System caused the System to be disconnected (as happened here), Plaintiff and Class members would be injured by the sudden and sustained lack of claims and payment processing by the Change Platform.

286. Change Health Defendants knew or should have known of the vulnerabilities of their System and of the significance of their inadequate security measures, including the reasonably foreseeable harm to Plaintiff and Class members from a System breach and disconnection. Change Health Defendants knew or should have known about the prevalence of ransomware attacks and data breaches in the healthcare sector. And Change

Health Defendants knew or should have known that their network security did not adequately safeguard the Services.

287. Change Health Defendants' duty to use reasonable care in securing and operating the System so as to protect against disconnection of the Change Platform also arises from the parties' relationship, as well as common law and federal law, and Change Health Defendants' own policies and promises regarding privacy and data security.

288. Change Health Defendants breached their duties to Plaintiff and Class members in numerous ways through their affirmative misfeasance, including by:

a. Creating, using, and implementing security systems, protocols, and practices that were insufficient to protect the System against reasonably foreseeable ransomware attacks;

b. Creating, using, and implementing systems, protocols, and practices that lacked redundancies and contingency protocols and were otherwise insufficient to ensure the continuity of the Change Platform and avoid sudden and sustained lack of claims and payment processing in the event of a breach of the System;

c. Creating, using, and implementing security systems, protocols, and practices that violated regulatory requirements and industry standard data security measures for the healthcare industry leading up to the Ransomware Attack;

d. Failing to comply with their own privacy and data security policies;

e. Failing to adequately monitor, evaluate, and ensure the security of the System;

f. Failing to have reasonably adequate contingency plans and backup systems to avoid sudden and sustained lack of claims and payment processing by the Change Platform; and

g. Failing to warn Plaintiff (directly or through their vendors) that the System was not adequately secured and/or that a reasonably foreseeable breach of the System could require disconnection and sudden and sustained loss of Services through the Change Platform.

289. Plaintiff and Class members would have been able to timely submit claims and receive timely payment for their healthcare services but for Change Health Defendants' wrongful and negligent breaches of their duties.

290. It was reasonably foreseeable to Change Health Defendants that a breach of the System could injure healthcare providers like Plaintiff and Class members whose claims and payments for healthcare services are routinely processed through the Change Platform and who reasonably rely on the timely and accurate processing of such claims and payments.

291. As a direct and proximate result of Change Health Defendants' negligence, Plaintiff and Class members have been injured and are entitled to damages in an amount to be proven at trial. Plaintiff's and Class members' damages include one or more of the following: missed payments for their healthcare services; delayed payments for their healthcare services; the costs of securing financing alternative to those missed or delayed payments; interest charges incurred; additional labor costs; expenses associated with and time spent hiring staff or vendors to troubleshoot the business disruption caused by Change

Health Defendants' shutdown of the Change Platform; expenses associated with and time spent researching and implementing new healthcare payment software and systems; expenses associated with and time spent attempting to manually submit claims and obtain payments that otherwise were to be processed through the Change Platform; late penalties assessed for untimely submission of claims; lost benefit of their bargains and overcharges for the Services; loss of the time-value of money, including but not limited to interest or other income, associated with the preceding injuries and damages.

292. Change Health Defendants' breaches of one or more of their duties was a substantial factor in causing harms, injuries, and damages to Plaintiff and Class members.

293. Change Health Defendants' conduct, as described above, was willful, wanton, reckless, oppressive, extreme, and outrageous, and displayed an entire want of care and a conscious and depraved indifference to the consequences of their conduct and warrants an award of punitive damages in an amount sufficient to punish the Change Health Defendants and deter others from like conduct.

COUNT II: NEGLIGENCE PER SE
(On Behalf of Plaintiff and the National Providers Class, or Alternatively, the Statewide Class, Against the Change Health Defendants)

294. Plaintiff repeats and realleges every allegation set forth in Paragraphs 1 to 281.

295. At all relevant times, each Change Health Defendant had an obligation to comply with applicable statutes and regulations, including Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1) and HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts

A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

296. Section 5 of the FTC prohibits "unfair . . . practices in or affecting commerce." The FTC has interpreted Section 5 to include as an unfair act or practice the failure by a business to employ reasonable security measures to secure access to their paid-for systems, despite representing otherwise.

297. The HIPAA Privacy and Security Rules require, *inter alia*, that Change Health Defendants maintain adequate data security systems to reduce the risk of data breaches and cyberattacks, adequately protect the PHI of patients, and ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted. *See, e.g.*, 45 C.F.R. § 164.306(a)(1).

298. Change Health Defendants violated Section 5 of the FTCA and HIPAA Privacy and Security Rules by failing to use reasonable security measures to secure access to their paid-for Change Platform, despite representing otherwise, including by not complying with applicable industry standards. Change Health Defendants' conduct was particularly unreasonable given the nature and amount of sensitive information they collect, maintain, and/or transfer as well as the nature of the Change Platform's business. Change Health Defendants' conduct was also unreasonable given the foreseeable consequences of a System breach to the continuity of the Services (given Change Health Defendants' lack of redundancies and contingency plans) and the resulting impact on Plaintiff and Class members as described above.

299. Defendants' violation of Section 5 of the FTCA and the HIPAA Privacy and Security Rules constitutes negligence per se.

300. Plaintiff and Class members are within the class of persons that Section 5 of the FTCA and HIPAA Privacy and Security Rules were intended to protect.

301. The harm suffered by Plaintiff and Class members as a result of the Ransomware Attack is the type of harm that Section 5 of the FTCA and HIPAA Privacy and Security Rules were intended to guard against.

302. It was reasonably foreseeable to Change Health Defendants that their failure to exercise reasonable care in securing the System would result in harm to Plaintiff and Class members due to not being able to timely submit claims for and not receiving timely payments for their healthcare services.

303. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Change Health Defendants' violation of Section 5 of FTCA and HIPAA Privacy and Security Rules. Plaintiff and Class members have been injured and are entitled to damages in an amount to be proven at trial. Plaintiff's and Class members' damages include one or more of the following: missed payments for their healthcare services; delayed payments for their healthcare services; the costs of securing financing alternative to those missed or delayed payments; interest charges incurred; additional labor costs; expenses associated with and time spent hiring staff or vendors to troubleshoot the business disruption caused by Change Health Defendants' shutdown of the Change Platform; expenses associated with and time spent researching and implementing new healthcare payment software and systems; expenses associated with and

time spent attempting to manually submit claims and obtain payments that otherwise were to be processed through the Change Platform; late penalties assessed for untimely submission of claims; lost benefit of their bargains and overcharges for the Services; loss of the time-value of money, including but not limited to interest or other income, associated with the preceding injuries and damages.

304. Change Health Defendants' conduct, as described above, was willful, wanton, reckless, oppressive, extreme, and outrageous, and displayed an entire want of care and a conscious and depraved indifference to the consequences of their conduct and warrants an award of punitive damages in an amount sufficient to punish the Change Health Defendants and deter others from like conduct.

COUNT III: BREACH OF CONTRACT (TFAP)
(On Behalf of Plaintiff and the National Provider Loan Assistance Sub-Class, or Alternatively, the Statewide Class, Against Defendants)

305. Plaintiff repeats and realleges every allegation set forth in Paragraphs 1 to 281.

306. Plaintiff brings this claim on behalf of itself and the National Provider Loan Assistance Sub-Class against all Defendants.

307. Plaintiff and the National Provider Loan Assistance Sub-Class entered into contracts with Defendants for the provision of interest-free and fee-free loans through the TFAP.

308. The TFAP contracts are between Providers and Change Healthcare Operations, LLC, as well as all "parents, affiliates, successors, and assigns" of Change Healthcare Operations, LLC.

309. TFAP contracts are governed by the laws of the state of Minnesota, and designate jurisdiction and venue as proper in the state of Minnesota, for the resolution of any dispute arising under the agreement.

310. The TFAP contracts include an integration clause providing that the terms of the contracts are the complete and final agreement between the parties.

311. Plaintiff and National Provider Loan Assistance Sub-Class members performed substantially all that was required of them under their contracts with Defendants, or they were excused from doing so.

312. Providers would not have entered these contracts with Defendants without understanding that repayment of TFAP loans would not be required of them until payments impacted during the service disruption period were processed.

313. A meeting of the minds occurred, as Plaintiff and the National Provider Loan Assistance Sub-Class agreed, among other things, to participate in TFAP in exchange for Defendants' agreement to provide loans while the Change Platform remained out of service.

314. The processing of payments impacted by the shutdown prior to repayment by Plaintiff and the National Provider Loan Assistance Sub-Class members were material aspects of the contracts.

315. Plaintiff and the National Provider Loan Assistance Sub-Class members read, reviewed, and/or relied on this contract provision and/or otherwise understood that Defendants would not demand repayment of TFAP loans until payments impacted during the service disruption were processed.

316. Defendants breached its promise by demanding repayment of TFAP loans before payments impacted during the service disruption were processed, and by threatening to offsetting claims payments for temporary funding repayments.

317. As a direct and proximate result of Defendants' breach of contract, Plaintiff and National Provider Loan Assistance Sub-Class members did not receive the full benefit of their bargain and instead were provided with a loan service that was less valuable than described in their contracts.

318. Plaintiff and National Provider Loan Assistance Sub-Class members are also being damaged because they are being forced to repay the loans before they have received the money due on outstanding claims payments impacted by the shutdown to repay those loans. Plaintiff and National Provider Loan Assistance Sub-Class members are thus being forced to consider obtaining alternate sources of funds, at higher interest rates than the TFAP loans, in order to cover the shortfall remaining as a result of the shutdown.

319. Accordingly, Plaintiff and National Provider Loan Assistance Sub-Class members have been injured by Defendants' breach of contract and are entitled to damages and/or restitution in an amount to be proven at trial.

320. Plaintiff and National Provider Loan Assistance Sub-Class members are also entitled to an injunction precluding Defendants' further demands for repayment of TFAP loans until payments impacted during the service disruption period have been processed.

COUNT IV: UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Nationwide Providers Class, or Alternatively, the Statewide Class, Against Change Health Defendants)

321. Plaintiff repeats and realleges every allegation set forth in Paragraphs 1 to 281.

322. This Count is pleaded on behalf of Plaintiff and the National Providers Class members.

323. Plaintiff and National Providers Class members conferred benefits on Change Health Defendants, both directly and indirectly, in the form of payments for the Services. Plaintiff and National Providers Class members further conferred benefits on UHG and UHCS through the provision of patient services to insureds covered by a UHG subsidiary health insurers prior to payment. Change Health Defendants had knowledge of the benefits conferred by Plaintiff and National Providers Class members and appreciated, and retained, such benefits.

324. In accepting payments from Plaintiff and National Providers Class members, Change Health Defendants should have used, in part, the monies Plaintiff and National Providers Class members paid to them, directly and indirectly, to pay the costs of industry standard cybersecurity, threat detection, and incident response measures, including a business continuity plan. In accepting payments from Plaintiff and National Providers Class members, Change Health Defendants should have used the monies Plaintiff and

National Providers Class members paid to them, directly and indirectly, to maintain a functioning Change Platform and Services. In failing to provide such cybersecurity and incident response measures, including maintaining a functioning Change Platform and Services, Change Health Defendants have been unjustly enriched at Plaintiff's and National Providers Class members' expense. Change Health Defendants had no justification for failing to provide adequate data security protections and failing to maintain a functioning Change Platform and Services, and retention of benefits would be unjust and morally wrong.

325. Because of Change Health Defendants' wrongful and inequitable conduct, including Change Health Defendants' shutdown of the Change Platform and Services, UHG and UHCS unjustly benefitted from and retained the value of Plaintiff's and National Providers Class members' provision of patient services to insureds covered by a UHG subsidiary health insurer before payment. UHG and UHCS thus unjustly retained and had use of, either temporarily or permanently, money and interest or other investment income earned thereon that should have been timely paid to Plaintiff and National Providers Class members for their provision of patient services. UHG and UHCS had no justification for this conduct, and retention of benefits would be unjust and morally wrong.

326. Plaintiff and National Providers Class members have suffered damages and harm because of Change Health Defendants' negligent, and unlawful, conduct, inactions, and omissions. Change Health Defendants should be required to disgorge all unlawful or inequitable benefits received from Plaintiff and National Providers Class members.

COUNT V: INTERFERENCE WITH PROSPECTIVE ECONOMIC ADVANTAGE, BUSINESS RELATIONSHIP, OR EXPECTANCY
(On Behalf of Plaintiff and the Nationwide Providers Class, or Alternatively, the Statewide Class, Against Change Health Defendants)

327. Plaintiff repeats and realleges every allegation set forth in Paragraphs 1 to 281.

328. At the time of the Ransomware Attack and outage, Plaintiff and Class members had ongoing business relationships or business expectancies with third parties. Plaintiff and Class members submitted claims through the Change Platform to these third parties with the expectation and understanding that their claims would be processed and they would be reimbursed in a timely fashion, or worked with the third parties to submit claims through the Change Platform.

329. Change Health Defendants knew or should have known about these relationships or expectancies due to the intentional integration of the Change Platform and the Services and processes with the third parties and their data systems. Indeed, the Change Platform is an indispensable link in the healthcare reimbursement process, enabling Plaintiff and Class members and these third party businesses to conduct business transactions, process claims, and exchange payments. Plaintiff and Class members relied on Change Health Defendants to ensure they could run and grow successful businesses.

330. Despite Change Health Defendants positioning the Change Platform as a linchpin of the nation's healthcare system and crucial to Plaintiff's and Class members' healthcare business operations, Change Health Defendants (1) failed to implement reasonable and adequate security controls to prevent the Ransomware Attack; (2) shut

down the Change Platform without an adequate substitute in place to ensure that Plaintiff could be paid for the vital health services they performed; and (3) failed to have adequate business continuity or disaster recovery plans and capabilities to quickly recover the Systems.

331. Change Health Defendants failed to act with reasonable care and intentionally engaged in wrongful conduct, including by violating Section 5 of FTCA and HIPAA Privacy and Security Rules. Change Health Defendants had ample knowledge of the requirements to implement reasonable data security under the FTCA and HIPAA, and knew of the increased risk to healthcare entities, as well as many recent high profile cybersecurity incidents at other healthcare partner and Provider companies.

332. As a result of Change Health Defendants' intentional and wrongful conduct, Change Health Defendants interfered with and disrupted the business relationships or expectancies between Plaintiff and Class members and the third-party businesses.

333. Change Health Defendants knew interference with Plaintiff and Class members' business relationships and expectancies was substantially certain to occur as a result of the Ransomware Attack and shutdown.

334. Change Health Defendants did not have any privilege or justification for their actions, and they were strangers to the business relationships between Plaintiff and the third parties with which they interfered.

335. As a direct and proximate cause of Change Health Defendants' wrongful conduct, Plaintiff and Class members have suffered damages as discussed herein, including loss of the ability to obtain prospective economic advantages from existing business

relationships. Plaintiff and Class members were unable to obtain payment for services rendered as a result of the Change Health Defendants' interference. Further, Plaintiff's and Class members' damages include one or more of the following: missed payments for their healthcare services; delayed payments for their healthcare services; the costs of securing financing alternative to those missed or delayed payments; interest charges incurred; additional labor costs; expenses associated with and time spent hiring staff or vendors to troubleshoot the business disruption caused by Change Health Defendants' shutdown of the Change Platform; expenses associated with and time spent researching and implementing new healthcare payment software and systems; expenses associated with and time spent attempting to manually submit claims and obtain payments that otherwise were to be processed through the Change Platform; late penalties assessed for untimely submission of claims; lost benefit of their bargains and overcharges for the Services; loss of the time-value of money, including but not limited to interest or other income, associated with the preceding injuries and damages.

COUNT VI: NEGLIGENT OMISSION
(On Behalf of Plaintiff and the National Providers Class, or Alternatively, the Statewide Class, Against the Change Health Defendants)

336. Plaintiff repeats and realleges every allegation set forth in Paragraphs 1 to 281.

337. Plaintiff and the National Providers Class bring this claim as to Change Health Defendants' statements and omissions after the Ransomware Attack and shutdown.

338. As alleged in greater detail above, Change Health Defendants omitted material information: (1) regarding the unsecure nature of their services; and (2) following

the Ransomware Attack, regarding the impact of the Ransomware Attack on the Change Platform and the timeline for when it would be back online. Specifically, Change Health Defendants omitted or otherwise failed to disclose that they: (1) lacked adequate data privacy practices, which rendered the Services unsecure and led to the Ransomware Attack; and (2) facts that clearly indicated that it would be months before the Change Platform was up and running at its previous capacity.

339. Change Health Defendants knowingly and deliberately failed to disclose (1) material weaknesses in Change's System, and (2) the true timeline for when the Change Platform would be back online, both of which good faith and common decency required them to disclose to Plaintiff and Class members.

340. Such omissions were material following the Ransomware Attack, when Plaintiff and members of the National Providers Class attempted to mitigate the harm imposed by Change Health Defendants' shutdown of the Change Platform.

341. Plaintiff and members of the National Providers Class would have taken different measures to mitigate their harm had Change Health Defendants provided truthful and accurate information about the duration of their intentional shutdown of the Change Platform.

342. Change Health Defendants knew that their data security obligations were particularly important given the substantial increase in cyber-attacks and/or ransomware attacks targeting healthcare entities that collect and store Private Information, preceding the date of the Ransomware Attack. Change Health Defendants were further aware in their industry that Providers and their affiliates are prime targets because of the sensitive

information they collect and store, including financial information of patients, login credentials, insurance information, medical records and diagnoses, and personal information of employees and patients—all extremely valuable on underground markets. Additionally, Change Health Defendants knew or should have known that they were at risk of experiencing the Ransomware Attack based on the substantial number of recent high profile cybersecurity incidents at other healthcare partner and provider companies. Indeed, in their SEC filings, Change Healthcare, Optum Insight, and UHG explicitly acknowledged the broad range of cybersecurity risks that they face. This knowledge is imputed to remaining Change Health Defendants as mutually owned and controlled corporate parent/subsidiaries.

343. Change Health Defendants knew that conveying accurate information about the impact of the Ransomware Attack on the Change Platform and the timeline for when it would be back online was particularly important to Plaintiff and National Providers Class members so they could make informed decisions and mitigate the harm they experienced as a direct result of the Change Platform shutdown. Indeed, Change Health Defendants knew how critical the Change Platform is to Plaintiff and National Providers Class members—whether they use the Change Platform directly or through third-party intermediaries—in the everyday course of their businesses, to (among many other vital services) submit and receive payment for healthcare services through the Change Platform. Change Health Defendants had exclusive knowledge of facts that clearly indicated that it would be months before the Change Platform was up and running at its capacity prior to the Ransomware Attack, but omitted or otherwise failed to convey that information to

Plaintiff and Class members. This knowledge is imputed to all Change Health Defendants as mutually owned and controlled corporate parent/subsidiaries.

344. As a direct and proximate result of Change Health Defendants' wrongful conduct, Plaintiff and National Providers Class members have suffered damages including one or more of the following: missed payments for their healthcare services; delayed payments for their healthcare services; the costs of securing financing alternative to those missed or delayed payments; interest charges incurred; additional labor costs; expenses associated with and time spent hiring staff or vendors to troubleshoot the business disruption caused by Change Health Defendants' shutdown of the Change Platform; expenses associated with and time spent researching and implementing new healthcare payment software and systems; expenses associated with and time spent attempting to manually submit claims and obtain payments that otherwise were to be processed through the Change Platform; late penalties assessed for untimely submission of claims; lost benefit of their bargains and overcharges for the Services; loss of the time-value of money, including but not limited to interest or other income, associated with the preceding injuries and damages.

COUNT VII: NEGLIGENT MISREPRESENTATION
(On Behalf of Plaintiff and the National Providers Class, or Alternatively, the Statewide Class, Against the Change Health Defendants)

345. Plaintiff repeats and realleges every allegation set forth in Paragraphs 1 to 281.

346. Plaintiff and the National Providers Class bring this claim as to Change Health Defendants' statements and omissions after the Ransomware Attack and shutdown.

347. As alleged in greater detail above, Change Health Defendants made numerous representations: (1) regarding the supposed secure nature of the Services; and (2) following the Ransomware Attack, regarding the impact of the Ransomware Attack on the Change Platform and the timeline for when it would be back online. Such representations were false because Change Health Defendants (1) lacked adequate data privacy practices, which rendered their services unsecure and led to the Ransomware Attack; and (2) had exclusive knowledge of facts that clearly indicated that it would be months before the Change Platform was up and running at its previous capacity.

348. Such representations were material to Plaintiff and Class members, who reasonably relied on Change Health Defendants' representations following the Ransomware Attack, when Plaintiff attempted to mitigate the harm imposed by Change Health Defendants' shutdown of the Change Platform.

349. Plaintiff and members of the National Providers Class would have taken different measures to mitigate their harm had Change Health Defendants provided truthful and accurate information about the duration of their intentional shutdown of the Change Platform.

350. Defendants intended for Plaintiff and Class members to rely on their representations both before and after the Ransomware Attack. In reliance on Defendants' representations, following the Ransomware Attack, Plaintiff relied on Change Health Defendants' representations when making crucial decisions/actions to mitigate the harm imposed by Change Health Defendants' shutdown of the Change Platform.

351. Change Health Defendants' representations were made with knowledge of their falsity, or at least with extreme disregard for their truth.

352. Change Health Defendants knew that their data security obligations were particularly important given the substantial increase in cyber-attacks and/or ransomware attacks targeting healthcare entities that collect and store Private Information, preceding the date of the Ransomware Attack. Change Health Defendants were further aware in their industry that Providers and their affiliates are prime targets because of the information they collect and store, including financial information of patients, login credentials, insurance information, medical records and diagnoses, and personal information of employees and patients—all extremely valuable on underground markets. Additionally, Change Health Defendants knew or should have known that they were at risk of experiencing the Ransomware Attack based on the substantial number of recent high profile cybersecurity incidents at other healthcare partner and provider companies. Indeed, in their SEC filings, Change Healthcare, Optum Insight, and UHG explicitly acknowledged the broad range of cybersecurity risks that they face. This knowledge is imputed to all Change Health Defendants as mutually owned and controlled corporate parent/subsidiaries.

353. Change Health Defendants knew that conveying accurate information about the impact of the Ransomware Attack on the Change Platform and the timeline for when it would be back online was particularly important to Plaintiff and National Providers Class members so they could make informed decisions and mitigate the harm they experienced as a direct result of the Change Platform shutdown. Indeed, Change Health Defendants knew how critical the Change Platform is to Plaintiff and National Providers Class

members—whether they use the Change Platform directly or through third-party intermediaries—in the everyday course of their businesses, to (among many other vital services) submit and receive payment for healthcare services provided by Plaintiff and National Providers Class members. Despite their statements to the contrary, Change Health Defendants had exclusive knowledge of facts that clearly indicated that it would be months before the Change Platform was up and running at its capacity prior to the Ransomware Attack. This knowledge is imputed to all Change Health Defendants as mutually owned and controlled corporate parent/subsidiaries.

354. As a direct and proximate result of Change Health Defendants' wrongful conduct, Plaintiff and National Providers Class members have suffered damages including one or more of the following: missed payments for their healthcare services; delayed payments for their healthcare services; the costs of securing financing alternative to those missed or delayed payments; interest charges incurred; additional labor costs; expenses associated with and time spent hiring staff or vendors to troubleshoot the business disruption caused by Change Health Defendants' shutdown of the Change Platform; expenses associated with and time spent researching and implementing new healthcare payment software and systems; expenses associated with and time spent attempting to manually submit claims and obtain payments that otherwise were to be processed through the Change Platform; late penalties assessed for untimely submission of claims; lost benefit of their bargains and overcharges for the Services; loss of the time-value of money, including but not limited to interest or other income, associated with the preceding injuries and damages.

COUNT VIII: PUBLIC NUISANCE
(On Behalf of Plaintiff and the National Providers Class, or Alternatively, the Statewide Class, Against the Change Health Defendants)

355. Plaintiff repeats and realleges every allegation set forth in Paragraphs 1 to 281.

356. The Change Health Defendants have substantially and unreasonably interfered with and endangered the public's rights to health, welfare, safety, peace, comfort, and ability to be free from disturbance and reasonable apprehension of danger to personal property by setting up, providing, managing, maintaining, operating, supervising, monitoring, securing, and controlling the Change Platform in a manner that made the platform unreasonably vulnerable to foreseeable attack and intrusion and to a sudden and sustained lack of timely and accurate claims and payment processing Services for Providers.

357. The Change Health Defendants' conduct was unreasonable in light of the known and foreseeable risks of a ransomware attack and industry standards for cybersecurity (including, e.g., the use of MFA). Further, the Change Health Defendants' conduct also violated standards set forth under federal law and regulations, rendering the conduct a per se nuisance.

358. As set forth above, at the time of the Ransomware Attack, the Change Platform was a critical linchpin in the country's healthcare services infrastructure. Huge swathes of the healthcare sector—e.g., 94% of hospitals, 100 million patients, and approximately 1/3 of all healthcare claims and payments—were dependent (knowingly or unknowingly) on the reliable operation of the Change Platform to timely and accurately

process multiple types of transactions needed to provide healthcare to patients throughout the U.S., including verification of insurance for new patients, verification of patient eligibility and coverage, prior authorizations, processing of insurance claims and appeals from denials of claims, electronic remittance advice, and payments from insurers.

359. Having actively worked to make their platform the backbone of healthcare operations across the country—both through direct contracts with Providers and by contracting with innumerable vendors that provide electronic services to Providers—the Change Health Defendants' unreasonably inadequate security systems and contingency planning is all the more egregious.

360. At all relevant times, the Change Health Defendants had control over the instrumentality that has caused the public nuisance at issue, namely the Change Platform and the System, as well as control over their own conduct that caused the public nuisance, namely the unreasonably insecure and lax manner in which they set up, provide, manage, maintain, operate supervise, monitor, secure, and control the Change Platform and System, including the multiple failures described in this Complaint.

361. The Change Health Defendants knew or reasonably should have known that the harm caused by their conduct outweighed any potential benefit of the use of the Change Platform in its inadequately secured state.

362. The public nuisance, and the economic and other harms to Plaintiff and Class members was reasonably foreseeable to the Change Health Defendants.

363. The Change Health Defendants' conduct caused, created, or was a substantial factor in causing the public nuisance at issue, namely a significant and substantial

interference with the public's common rights to health, welfare, safety, peace, comfort, and ability to be free from disturbance and reasonable apprehension of danger to personal property. As set forth above, following the Ransomware Attack and the sudden and sustained loss of services from the Change Platform, the ability of patients to receive healthcare was substantially disrupted, compromised, and endangered throughout the country, including (a) when Providers were unable to verify coverage, benefits, or prescriptions for patients, resulting in healthcare being delayed, denied, or inaccessible to patients, (b) when Providers were forced to cut back on hours, staff, and supplies that otherwise would have been available for patient care due to lack of timely and reliable processing of claims and payments, and (c) when Providers were forced to divert staff and resources from patient care to instead address the lack of Services from the Change Platform (e.g., trying to process claims and verifications off-platform, trying to secure other sources of cash, and trying to switch to another platform).

364. As Providers, Plaintiff and Class members suffered special economic injuries distinct from the general harm to healthcare suffered by the public at large (and also distinct from the privacy harms suffered by patients whose Private Information was compromised). As set forth above, as a direct and proximate result of Change Health Defendants' conduct, Plaintiff and Class members have been injured and are entitled to damages in an amount to be proven at trial. Plaintiff's and Class members' damages include one or more of the following: missed payments for their healthcare services; delayed payments for their healthcare services; the costs of securing financing alternative to those missed or delayed payments; interest charges incurred; additional labor costs; expenses associated with and

time spent hiring staff or vendors to troubleshoot the business disruption caused by Change Health Defendants' shutdown of the Change Platform; expenses associated with and time spent researching and implementing new healthcare payment software and systems; expenses associated with and time spent attempting to manually submit claims and obtain payments that otherwise were to be processed through the Change Platform; late penalties assessed for untimely submission of claims; lost benefit of their bargains and overcharges for the Services; loss of the time-value of money, including but not limited to interest or other income, associated with the preceding injuries and damages.

365. Plaintiff and Class members are entitled to appropriate relief to abate the public nuisance, including injunctive relief requiring the Change Health Defendants to implement appropriate security measures and contingency plans to protect critical infrastructure technology and Private Information and to avoid further sudden and sustained service outages, injunctive relief requiring the Change Health Defendants to create and robustly fund and staff a system to promptly resolve claim and payment backlogs and assist Providers with information and financial support needed to respond to ongoing questions and/or "late" claim penalties, and injunctive relief forgiving (in whole or part) loans or advances made by Defendants to Plaintiff and Class members in the wake of the Ransomware Attack.

366. Plaintiff and the Class members request all the relief to which they are entitled in their own right with respect to the distinct special damages they have suffered, including actual and compensatory damages in an amount to be determined at trial. Plaintiff and the Class members further request declaratory and injunctive relief providing for the

abatement of the public nuisance Defendants have created, payment to Plaintiff and the Class members of monies to abate the public nuisance, and an order enjoining Defendants from future conduct contributing to the public nuisance described above.

COUNT IX: VIOLATION OF THE MINNESOTA PROTECTION OF CONSUMER FRAUD ACT
Minn. Stat. §§ 325F.68-325F.70
(On Behalf of Plaintiff and the National Providers Class, or alternatively, the Minnesota State Class, Against the Change Health Defendants)

367. Plaintiff repeats and realleges every allegation set forth in Paragraphs 1 to 281.

368. Under the Minnesota Protection of Consumer Fraud Act ("MPCFA"), and enforced through § 8.31, it is unlawful for any person to commit a fraud, false pretense, false promise, misrepresentation, misleading statement, or deceptive practice with the intent that others rely thereon in connection with the sale of any merchandise.

369. Plaintiff and National Providers Class members are considered "persons" for the purpose of the MPCFA and § 8.31.

370. Change Health Defendants committed frauds, false pretenses, false promises, misrepresentations, misleading statements, or deceptive practices, including but not limited to the following:

a. Prior to the shutdown, Change Health Defendants knowingly and willingly misrepresented, through statements and omissions, that their network maintained adequate protections and maintained data in a HIPAA-compliant manner to induce Plaintiff and National Providers Class members to use and rely on Change Health Defendants' services.

Plaintiff's and Class members' decision to trust Change Health Defendants with their processing needs was based on Change Health Defendants' statements that Change Health Defendants would take adequate security precautions and maintain industry standard cybersecurity measures, and omissions that Change Health Defendants maintained weak data security that failed to comply with the law.

b. During the shutdown, Change Health Defendants knowingly and willingly misrepresented, through statements and omissions, the extent and impact of the shutdown. Change Health Defendants did so with the intent to deceive Plaintiff and National Providers Class members into believing that the Change Platform would return to functionality quickly.

371. Change Health Defendants did so with the intent that others rely thereon, whether or not any person was in fact misled.

372. Change Health Defendants did so in connection with the sale of merchandise.

373. Plaintiff and National Providers Class members were injured by Change Health Defendants' conduct:

a. As a direct and proximate result of Change Health Defendants' wrongful conduct, Plaintiff and National Providers Class members have suffered damages including one or more of the following: missed payments for their healthcare services; delayed payments for their healthcare services; the costs of securing financing alternative to those missed or delayed payments; interest charges incurred; additional labor costs; expenses

associated with and time spent hiring staff or vendors to troubleshoot the business disruption caused by Change Health Defendants' shutdown of the Change Platform; expenses associated with and time spent researching and implementing new healthcare payment software and systems; expenses associated with and time spent attempting to manually submit claims and obtain payments that otherwise were to be processed through the Change Platform; late penalties assessed for untimely submission of claims; lost benefit of their bargains and overcharges for the Services; loss of the time-value of money, including but not limited to interest or other income, associated with the preceding injuries and damages.

b. Moreover, as a direct and proximate result of Change Health Defendants' misleading statements and omissions during the shutdown, Plaintiff and National Providers Class members incurred additional financial damages, the extent of which is not yet fully known and continues to impact Plaintiff and National Providers Class members.

374. There is a causal relationship between Plaintiff's and Class members' loss and Change Health Defendants' actions:

a. But for Change Health Defendants' failure to employ reasonable security measures, in violation of the law, and despite representing otherwise, the Change Platform would not have been shut down, and Plaintiff and

National Providers Class members would not have suffered injuries and incurred damages.

b. But for Change Health Defendants' misleading statements and omissions regarding the efficacy of Change Health Defendants' security measures, Plaintiff and National Providers Class members would not have relied on Change Health Defendants for their clearinghouse services and would not have suffered injuries and incurred damages.

c. But for Change Health Defendants' misleading statements and omissions regarding the duration and extent of the shutdown, Plaintiff and National Providers Class members would not have incurred additional costs associated with mitigating the damage caused by Change Health Defendants.

d. Thus, Plaintiff and National Providers Class members relied on Change Health Defendants actions.

375. There is a public benefit in holding Change Health Defendants liable for their fraudulent, misleading, and deceptive actions. Change Health Defendants directed their numerous misleading statements and omissions at the consuming public and the marketplace. Change Health Defendants' misleading statements and omissions were widely covered in the media and relied on by providers. This prevented providers, insurers, and EHR vendors from making informed decisions during the shutdown, thereby impacting the consumer decision-making process. There is a public benefit in holding Change Health Defendants liable for their misleading statements and omissions.

COUNT X: DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the National Providers Class, or Alternatively, the Statewide Class, Against the Change Health Defendants)

376. Plaintiff repeats and realleges every allegation set forth in Paragraphs 1 to 281.

377. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

378. An actual controversy has arisen in the wake of the Ransomware Attack regarding Defendants' present and prospective common law and other duties to reasonably safeguard the networks that provide services that Plaintiff and Class members rely on for Services, and whether Change Health Defendants are currently maintaining data security measures adequate to prevent further ransomware attacks and ensure a functioning Change Platform, which is a lynchpin of Providers' payment practices.

379. Another ransomware attack would likely result in Change Health Defendants disconnecting the Change Platform again, causing further injuries to Plaintiff and Class members.

380. Pursuant to the Declaratory Judgment Act, Plaintiff and Class members seek a declaration that: (a) Change Health Defendants' existing data security measures do not comply with their obligations and duties of care; and (b) in order to comply with their

obligations and duties of care, (1) Change Health Defendants must have policies and procedures in place to ensure the Change Platform and the System maintain reasonable, industry-standard security measures, including, but not limited to, those listed in this Complaint, and must comply with those policies and procedures; (2) Change Health Defendants must implement and maintain reasonable, industry-standard security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Change Health Defendants' System on a periodic basis, and ordering Change Health Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training their security personnel regarding any new or modified procedures;

d. Encrypting Private Information and segmenting critical technology and Private Information by, among other things, creating firewalls and access controls so that if one area of the System is compromised, cybercriminals cannot gain access to other portions of the System;

e. Purging, deleting, and destroying in a reasonable and secure manner Providers' patients' Private Information not necessary to perform essential business functions;

f. Conducting regular database scanning and security checks;

g. Conducting regular employee education regarding best security practices;

h. Implementing MFA and the principle of least privilege to combat system-wide ransomware attacks; and

i. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a ransomware attack when it occurs and what to do in response.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, on behalf of itself and Class members set forth herein, respectfully request the following relief:

(a) That the Court certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, appoint Plaintiff as class representative and Plaintiff's counsel as Class Counsel;

(b) That the Court grant permanent injunctive relief to prohibit and prevent Defendants from continuing to engage in the unlawful acts, omissions, and practices described herein;

(c) That the Court award Plaintiff and Class members compensatory, consequential, and general damages, including nominal damages as appropriate, for each count as allowed by law in an amount to be determined at trial;

(d) That the Court award statutory damages, trebled, and/or punitive or exemplary damages, to the extent permitted by law;

(e) That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of their unlawful acts, omissions, and practices;

(f) That Plaintiff be granted the declaratory and injunctive relief sought herein;

(g) That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses; and

(h) That the Court award pre-and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial in the instant action.

Dated: March 14, 2025

s/Daniel E. Gustafson

Daniel E. Gustafson (#202241)
Amanda M. Williams (#341691)
David A. Goodwin (#386715)
Mary M. Nikolai (#400354)
GUSTAFSON GLUEK PLLC
120 South 6th Street, Suite 2600
Minneapolis, MN 55402
612-333-8844
dgustafson@gustafsongluek.com
awilliams@gustafsongluek.com
dgoodwin@gustafsongluek.com
mnikolai@gustafsongluek.com

Overall Lead Counsel

E. Michelle Drake, Bar No. 0387366
BERGER MONTAGUE
1229 Tyler Street NE, Suite 205
Minneapolis, MN 55413
Telephone: (612) 594-5933
emdrake@bm.net

Norman E. Siegel
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Telephone: (816) 714-7100
siegel@stuevesiegel.com

Warren Burns
BURNS CHAREST LLP
900 Jackson Street, Suite 500
Dallas, TX 75202
(469) 458-9890
wburns@burnscharest.com

Provider Track Co-Lead Counsel

Jennifer Scullion
SEEGER WEISS LLP
100 Church Street
New York, NY 10007
(212) 584-0700
jscullion@seegerweiss.com

Charles J. LaDuca
CUNEO GILBERT & LADUCA, LLP
4725 Wisconsin Avenue, Suite 200
Washington, D.C. 20016
(202) 789-3960
charlesl@cuneolaw.com

Adam Polk
GIRARD SHARP
601 California St., Suite 1400
San Francisco, CA 94108
(415) 544-6280
apolk@girardsharp.com

Melissa Gardner
LIEFF CABRASER HEIMANN & BERNSTEIN
275 Battery Street, 29th Floor
San Francisco, CA 94111
(415) 956-1000

mgardner@lchb.com

Nick Murphy
HAUSFELD LLP
888 16th Street N.W., Suite 300
Washington, D.C. 2006
(202) 540-7200
nmurphy@hausfeld.com

David Berger
GIBBS LAW GROUP LLP
1111 Broadway, Suite 2100
Oakland, CA 94607
(510) 350-9713
dmb@classlawgroup.com

Deepali Brahmbhatt
DEVLIN LAW FIRM LLC
1526 Gilpin Avenue
Wilmington, DE 19806
(302) 449-9010
dbrahmbhatt@devlinlawfirm.com

Jack Meyerson
MEYERSON & MILLER
1600 Market Street, Suite 1305
Philadelphia, PA 19103
(215) 972-1376
jmeyerson@meyersonlawfirm.com

Jeff Ostrow
KOPELOWITZ OSTROW FERGUSON
WEISELBERG GILBERT
1 West Las Olas Blvd., 5th Floor
Fort Lauderdale, FL 33301
(954) 525-4100
ostrow@kolawyers.com

Thomas A. Zimmerman, Jr.
ZIMMERMAN LAW OFFICES, P.C.
77 W. Washington Street, Suite 1220
Chicago, IL 60602
Telephone: (312) 440-0020

tom@attorneyzim.com

Jan Conlin
CIRESI CONLIN LLP
225 South 6th Street, Suite 4600
Minneapolis, MN 55402
(612) 361-8200
jmc@ciresiconlin.com

Stephen J. Herman
FISHMAN HAYGOOD L.L.P.
201 St. Charles Avenue, Suite 4600
New Orleans, LA 70170
(504) 556-5541
sherman@fishmanhaygood.com

Provider Track Plaintiff Steering Committee